Ref. 4

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－222618

(43)公開日　平成10年(1998)８月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｂ
			Ｄ
			Ｔ
19/10		Ｈ０４Ｍ　15/00	Ｚ
19/00		17/02	Ａ

審査請求　未請求　請求項の数28　ＯＬ　（全 28 頁）　最終頁に続く

(21)出願番号　特願平9－19399

(22)出願日　平成９年(1997)１月31日

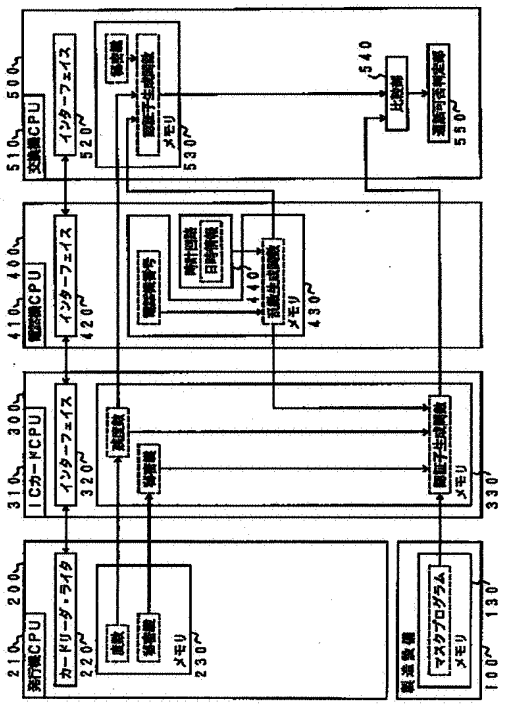
(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　西岡　満
神奈川県川崎市幸区柳町70番地　東芝インテリジェントテクノロジ株式会社内

(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　ＩＣカード及びＩＣカード処理システム

(57)【要約】
【課題】セキュリティの要となる秘密情報が漏洩しにくいＩＣカード処理システムを提供すること
【解決手段】ＩＣカード（２００）、このＩＣカードを取り扱う端末（３００）、及びこの端末を監視するホスト（４００）を有するＩＣカード処理システムにおいて、前記ＩＣカード中で、外部への読み出しが禁止されたキーデータ及び前記端末からの端末データから第１の認証データを生成し、前記端末中で、端末固有データから乱数データを生成し、前記ホスト中で、前記キーデータ及び前記端末からの乱数データから第２の認証データを生成し、この第２の認証データと前記ＩＣカード中で生成され前記端末を介して供給される第２の認証データとを比較してＩＣカードの真偽を判別することを特徴とするＩＣカード処理システム。



【特許請求の範囲】

【請求項１】各種演算処理を実行する集積回路を有するＩＣカードにおいて、

この集積回路が、

外部との間で各種データの受け渡しを行うデータ入出力手段と、

外部への読み出しが禁止されたキーデータを記憶する記憶手段と、

前記キーデータ及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、

を備えたことを特徴とするＩＣカード。

【請求項２】各種演算処理を実行する集積回路を有するＩＣカードにおいて、

この集積回路が、

外部との間で各種データの受け渡しを行うデータ入出力手段と、

プリペイドカードとしての価値を示す度数データを記憶する第１の記憶手段と、

外部への読み出しが禁止されたキーデータを記憶する第２の記憶手段と、

前記度数データ、キーデータ、及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、

を備えたことを特徴とするＩＣカード。

【請求項３】各種演算処理を実行する集積回路を有するＩＣカード、このＩＣカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するＩＣカード処理システムにおいて、

前記ＩＣカードに設けられた集積回路が、

前記端末装置との間で各種データの受け渡しを行う第１のデータ入出力手段と、

外部への読み出しが禁止されたキーデータを記憶する第１の記憶手段と、

この第１の記憶手段に記憶されたキーデータ、及び前記端末装置から供給される端末データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、

を備え、

前記端末装置が、

前記ＩＣカード及び前記ホスト装置との間で各種データの受け渡しを行う第２のデータ入出力手段と、

この端末装置の端末固有データを記憶する第２の記憶手段と、

この第２の記憶手段に記憶された端末固有データを基にして乱数データを生成する乱数データ生成手段と、

を備え、

前記ホスト装置が、

前記端末装置との間で各種データの受け渡しを行う第３のデータ入出力手段と、

前記第１の記憶手段に記憶されたものと同じキーデータを記憶する第３の記憶手段と、

この第３の記憶手段に記憶されたキーデータ及び前記端末装置から供給される乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、

この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、

この比較手段による比較結果から、前記端末装置で取り扱われるＩＣカードの真偽を判別し、前記端末装置で取り扱われるＩＣカードによる各種処理の実行の可否を判定する判定手段と、

を備えたことを特徴とするＩＣカード処理システム。

【請求項４】前記ＩＣカードに設けられた集積回路が、プリペイドカードとしての価値を示す度数データを記憶する第４の記憶手段を備え、

前記第１の認証データ生成手段が、前記第１の記憶手段に記憶されたキーデータ、前記第４の記憶手段に記憶された度数データ、及び前記端末装置から供給される乱数データを基にして認証データを生成し、

前記第２の認証データ生成手段が、前記第３の記憶手段に記憶されたキーデータ、前記第４の記憶手段に記憶され前記端末装置を介して供給される度数データ、及び前記端末装置から供給される乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する、

ことを特徴とする請求項３に記載のＩＣカード処理システム。

【請求項５】前記端末装置が、日時データを得るための時計を備え、

前記乱数データ生成手段が、前記第２の記憶手段に記憶された端末固有データ、及び前記時計から得られる日時データを基にして乱数データを生成する、

ことを特徴とする請求項３に記載のＩＣカード処理システム。

【請求項６】前記ＩＣカードの集積回路に対して前記キーデータを書き込みＩＣカードを発行するカード発行装置を含むことを特徴とする請求項３又は請求項５に記載のＩＣカード処理システム。

【請求項７】前記ＩＣカードの集積回路に対して前記キーデータ及び前記度数データを書き込みＩＣカードを発行するカード発行装置を含むことを特徴とする請求項４に記載のＩＣカード処理システム。

【請求項８】各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するＩＣカード、このＩＣカードの集積回路に記憶された度数データの度数と引き替えに通話が可能な電話機、及びこの電話機と通信対象となる他の電

話機とを接続する交換機を有するＩＣカード処理システムにおいて、
前記ＩＣカードに設けられた集積回路が、
前記電話機との間で各種データの受け渡しを行う第１のデータ入出力手段と、
前記度数データを記憶する第１の記憶手段と、
外部への読み出しが禁止されたキーデータを記憶する第２の記憶手段と、
前記第１の記憶手段に記憶された度数データ、前記第２の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、
を備え、
前記電話機が、
前記ＩＣカード及び前記交換機との間で各種データの受け渡しを行う第２のデータ入出力手段と、
電話機固有の電話機固有データを記憶する第３の記憶手段と、
日時データを得るための時計と、
前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、
を備え、
前記交換機が、
前記電話機との間で各種データの受け渡しを行う第３のデータ入出力手段と、
前記第２の記憶手段に記憶されたものと同じキーデータを記憶する第４の記憶手段と、
前記第１の記憶手段に記憶され前記電話機を介して供給される度数データ、前記第４の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、
この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、
この比較手段による比較結果から、前記電話機で取り扱われるＩＣカードの真偽を判別し、前記電話機で取り扱われるＩＣカードによる通話の可否を判定する判定手段と、
を備えたことを特徴とするＩＣカード処理システム。
【請求項９】各種演算処理を実行する集積回路を有するＩＣカードにおいて、
この集積回路が、
外部との間で各種データの受け渡しを行うデータ入出力手段と、
このＩＣカード固有のカード固有データを記憶する第１の記憶手段と、
外部への読み出しが禁止されたキーデータを記憶する第２の記憶手段と、
前記カード固有データ、前記キーデータ、及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、
を備えたことを特徴とするＩＣカード。
【請求項１０】各種演算処理を実行する集積回路を有するＩＣカードにおいて、
この集積回路が、
外部との間で各種データの受け渡しを行うデータ入出力手段と、
プリペイドカードとしての価値を示す度数データを記憶する第１の記憶手段と、
このＩＣカード固有のカード固有データを記憶する第２の記憶手段と、
外部への読み出しが禁止されたキーデータを記憶する第３の記憶手段と、
前記度数データ、前記カード固有データ、前記キーデータ、及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、
を備えたことを特徴とするＩＣカード。
【請求項１１】前記キーデータとして異なる複数のキーデータを設定し、状況に応じてこれら複数のキーデータを使い分けることを特徴とする請求項９又は１０に記載のＩＣカード。
【請求項１２】各種演算処理を実行する集積回路を有するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、及びこのＩＣカードを取り扱うカード処理装置を有するＩＣカード処理システムにおいて、
前記発行装置が、
前記ＩＣカードの集積回路に対して、ＩＣカード固有のカード固有データ及びキーデータを書き込む書込手段を備え、
前記ＩＣカードに設けられた集積回路が、
前記カード処理装置との間で各種データの受け渡しを行う第１のデータ入出力手段と、
前記カード固有データを記憶する第１の記憶手段と、
前記キーデータを外部への読み出しを禁止した状態で記憶する第２の記憶手段と、
前記カード固有データ、前記キーデータ、及び前記カード処理装置から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、
を備え、
前記カード処理装置が、
前記ＩＣカードとの間で各種データの受け渡しを行う第２のデータ入出力手段と、
このカード処理装置のカード処理装置固有データを記憶

する第３の記憶手段と、
この第３の記憶手段に記憶されたカード処理装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、
前記第２の記憶手段に記憶されたものと同じキーデータを記憶する第４の記憶手段と、
前記第１の記憶手段に記憶されＩＣカードから供給されるカード固有データ、前記第４の記憶手段に記憶されたキーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、
この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記ＩＣカードから供給される認証データとを比較する比較手段と、
この比較手段による比較結果から、前記カード処理装置で取り扱われるＩＣカードの真偽を判別し、前記カード処理装置で取り扱われるＩＣカードによる各種処理の実行の可否を判定する判定手段と、
を備えたことを特徴とするＩＣカード処理システム。

【請求項１３】各種演算処理を実行する集積回路を有するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、このＩＣカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するＩＣカード処理システムにおいて、
前記発行装置が、
前記ＩＣカードの集積回路に対して、ＩＣカード固有のカード固有データ及びキーデータを書き込む書込手段を備え、
前記ＩＣカードに設けられた集積回路が、
前記カード処理装置との間で各種データの受け渡しを行う第１のデータ入出力手段と、
前記カード固有データを記憶する第１の記憶手段と、
前記キーデータを外部への読み出しを禁止した状態で記憶する第２の記憶手段と、
前記カード固有データ、前記キーデータ、及び前記端末装置から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、
を備え、
前記端末装置が、
前記ＩＣカード及び前記ホスト装置との間で各種データの受け渡しを行う第２のデータ入出力手段と、
この端末装置の端末固有データを記憶する第３の記憶手段と、
この第３の記憶手段に記憶された端末固有データを基にして前記乱数データを生成する乱数データ生成手段と、
を備え、
前記ホスト装置が、
前記端末装置との間で各種データの受け渡しを行う第３のデータ入出力手段と、
前記第２の記憶手段に記憶されたものと同じキーデータを記憶する第４の記憶手段と、
前記第１の記憶手段に記憶されＩＣカードから供給されるカード固有データ、前記第４の記憶手段に記憶されたキーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、
この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、
この比較手段による比較結果から、前記端末装置で取り扱われるＩＣカードの真偽を判別し、前記端末装置で取り扱われるＩＣカードによる各種処理の実行の可否を判定する判定手段と、
を備えたことを特徴とするＩＣカード処理システム。

【請求項１４】前記ＩＣカードに設けられた集積回路が、プリペイドカードとしての価値を示す度数データを記憶する第５の記憶手段を備え、
前記第１の認証データ生成手段が、前記第１の記憶手段に記憶されたカード固有データ、前記第２の記憶手段に記憶されたキーデータ、前記第５の記憶手段に記憶された度数データ、及び前記端末装置から供給される乱数データを基にして認証データを生成し、
前記第２の認証データ生成手段が、前記第１の記憶手段に記憶され前記端末装置を介して供給されるカード固有データ、前記第４の記憶手段に記憶されたキーデータ、前記第５の記憶手段に記憶され前記端末装置を介して供給される度数データ、及び前記端末装置から供給される乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する、
ことを特徴とする請求項１３に記載のＩＣカード処理システム。

【請求項１５】前記端末装置が、日時データを得るための時計を備え、
前記乱数データ生成手段が、前記第３の記憶手段に記憶された端末固有データ、及び前記時計から得られる日時データを基にして乱数データを生成する、
ことを特徴とする請求項１３に記載のＩＣカード処理システム。

【請求項１６】各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、このＩＣカードの集積回路に記憶された度数データの度数と引き替えに通話が可能な電話機、及びこの電話機と通信対象となる他の電話機とを接続する交換機を有するＩＣカード

処理システムにおいて、
前記発行装置が、
前記ＩＣカードの集積回路に対して、ＩＣカード固有のカード固有データ、度数データ、及びキーデータを書き込む書込手段を備え、
前記ＩＣカードに設けられた集積回路が、
前記電話機との間で各種データの受け渡しを行う第１のデータ入出力手段と、
前記カード固有データを記憶する第１の記憶手段と、
前記度数データを記憶する第２の記憶手段と、
前記キーデータを外部への読み出しを禁止した状態で記憶する第３の記憶手段と、
前記第１の記憶手段に記憶されたカード固有データ、前記第２の記憶手段に記憶された度数データ、前記第３の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、
を備え、
前記電話機が、
前記ＩＣカード及び前記交換機との間で各種データの受け渡しを行う第２のデータ入出力手段と、
電話機固有の電話機固有データを記憶する第４の記憶手段と、
日時データを得るための時計と、
前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、
を備え、
前記交換機が、
前記電話機との間で各種データの受け渡しを行う第３のデータ入出力手段と、
前記第３の記憶手段に記憶されたものと同じキーデータを記憶する第５の記憶手段と、
前記第１の記憶手段に記憶され前記電話機を介して供給されるカード固有データ、前記第２の記憶手段に記憶され前記電話機を介して供給される度数データ、前記第５の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、
この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、
この比較手段による比較結果から、前記電話機で取り扱われるＩＣカードの真偽を判別し、前記電話機で取り扱われるＩＣカードによる通話の可否を判定する判定手段と、
を備えたことを特徴とするＩＣカード処理システム。
【請求項１７】前記キーデータとして異なる複数のキーデータを設定し、状況に応じてこれら複数のキーデータを使い分けることを特徴とする請求項１２、請求項１３、又は請求項１６に記載のＩＣカード処理システム。
【請求項１８】各種演算処理を実行する集積回路を有するＩＣカードにおいて、
この集積回路が、
外部との間で各種データの受け渡しを行うデータ入出力手段と、
このＩＣカード固有のカード固有データを記憶する第１の記憶手段と、
外部への読み出しが禁止されたものであって、前記カード固有データから生成されるカード固有のカード固有キーデータを記憶する第２の記憶手段と、
前記カード固有キーデータ及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、
を備えたことを特徴とするＩＣカード。
【請求項１９】各種演算処理を実行する集積回路を有するＩＣカードにおいて、
この集積回路が、
外部との間で各種データの受け渡しを行うデータ入出力手段と、
プリペイドカードとしての価値を示す度数データを記憶する第１の記憶手段と、
このＩＣカード固有のカード固有データを記憶する第２の記憶手段と、
外部への読み出しが禁止されたものであって、前記カード固有データから生成されるカード固有のカード固有キーデータを記憶する第３の記憶手段と、
前記度数データ、カード固有キーデータ、及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、
を備えたことを特徴とするＩＣカード。
【請求項２０】前記カード固有キーデータとして異なる複数のカード固有キーデータを設定し、状況に応じてこれら複数のカード固有キーデータを使い分けることを特徴とする請求項１８又は１９に記載のＩＣカード。
【請求項２１】各種演算処理を実行する集積回路を有するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、及びこのＩＣカードを取り扱うカード処理装置を有するＩＣカード処理システムにおいて、
前記発行装置が、
キーデータを記憶する第１の記憶手段と、
前記キーデータ及びＩＣカードに対して付与されるＩＣカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第１のカード固有キーデータ生成手段と、
前記ＩＣカードの集積回路に対して、前記カード固有デ

ータ及び前記カード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、
前記ＩＣカードに設けられた集積回路が、
前記カード処理装置との間で各種データの受け渡しを行う第１のデータ入出力手段と、
前記カード固有データを記憶する第２の記憶手段と、
前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第３の記憶手段と、
前記カード固有キーデータ及び前記カード処理装置から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、
を備え、
前記カード処理装置が、
前記ＩＣカードとの間で各種データの受け渡しを行う第２のデータ入出力手段と、
このカード処理装置のカード処理装置固有データを記憶する第４の記憶手段と、
この第４の記憶手段に記憶されたカード処理装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、
前記第１の記憶手段に記憶されたものと同じキーデータを記憶する第５の記憶手段と、
この第５の記憶手段に記憶されたキーデータ、及び前記第２の記憶手段に記憶され前記ＩＣカードを介して供給されるカード固有データに基づき、前記第１のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第２のカード固有キーデータ生成手段と、
前記第２のカード固有キーデータ生成手段により生成されるカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、
この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記ＩＣカードから供給される認証データとを比較する比較手段と、
この比較手段による比較結果から、前記カード処理装置で取り扱われるＩＣカードの真偽を判別し、前記カード処理装置で取り扱われるＩＣカードによる各種処理の実行の可否を判定する判定手段と、
を備えたことを特徴とするＩＣカード処理システム。
【請求項２２】各種演算処理を実行する集積回路を有するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、このＩＣカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するＩＣカード処理システムにおいて、
前記発行装置が、
キーデータを記憶する第１の記憶手段と、
前記キーデータ及びＩＣカードに対して付与されるＩＣカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第１のカード固有キーデータ生成手段と、
前記ＩＣカードの集積回路に対して、前記カード固有データ及び前記第１のカード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、
前記ＩＣカードに設けられた集積回路が、
前記端末装置との間で各種データの受け渡しを行う第１のデータ入出力手段と、
前記カード固有データを記憶する第２の記憶手段と、
前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第３の記憶手段と、
前記カード固有キーデータ及び前記端末装置から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、
を備え、
前記端末装置が、
前記ＩＣカードとの間で各種データの受け渡しを行う第２のデータ入出力手段と、
この端末装置の端末固有データを記憶する第４の記憶手段と、
この第４の記憶手段に記憶された端末装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、
前記ホスト装置が、
前記端末装置との間で各種データの受け渡しを行う第３のデータ入出力手段と、
前記第１の記憶手段に記憶されたものと同じキーデータを記憶する第５の記憶手段と、
この第５の記憶手段に記憶されたキーデータ、及び前記第２の記憶手段に記憶され前記ＩＣカードを介して供給されるカード固有データに基づき、前記第１のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第２のカード固有キーデータ生成手段と、
前記第２のカード固有キーデータ生成手段により生成されたカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、
この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、
この比較手段による比較結果から、前記端末装置で取り扱われるＩＣカードの真偽を判別し、前記端末装置で取り扱われるＩＣカードによる各種処理の実行の可否を判定する判定手段と、

を備えたことを特徴とするＩＣカード処理システム。

【請求項２３】前記ＩＣカードに設けられた集積回路が、プリペイドカードとしての価値を示す度数データを記憶する第６の記憶手段を備え、

前記第１の認証データ生成手段が、前記第３の記憶手段に記憶されたカード固有キーデータ、前記第６の記憶手段に記憶された度数データ、及び前記端末装置から供給される乱数データを基にして認証データを生成し、

前記第２の認証データ生成手段が、前記第２のカード固有キーデータ生成手段により生成されるカード固有キーデータ、前記第６の記憶手段に記憶され前記端末装置を介して供給される度数データ、及び前記端末装置から供給される乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する、

ことを特徴とする請求項２２に記載のＩＣカード処理システム。

【請求項２４】前記端末装置が、日時データを得るための時計を備え、

前記乱数データ生成手段が、前記第４の記憶手段に記憶された端末固有データ、及び前記時計から得られる日時データを基にして乱数データを生成する、

ことを特徴とする請求項２４に記載のＩＣカード処理システム。

【請求項２５】各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、このＩＣカードの集積回路に記憶された度数データの度数と引き替えに通話が可能な電話機、及びこの電話機と通信対象となる他の電話機とを接続する交換機を有するＩＣカード処理システムにおいて、

前記発行装置が、

キーデータを記憶する第１の記憶手段と、

前記キーデータ及びＩＣカードに対して付与されるＩＣカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第１のカード固有キーデータ生成手段と、

前記ＩＣカードの集積回路に対して、前記カード固有データ及び前記第１のカード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、

前記ＩＣカードに設けられた集積回路が、

前記電話機との間で各種データの受け渡しを行う第１のデータ入出力手段と、

前記カード固有データを記憶する第２の記憶手段と、

前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第３の記憶手段と、

前記カード固有キーデータ及び前記電話機から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、

を備え、

前記電話機が、

前記ＩＣカードとの間で各種データの受け渡しを行う第２のデータ入出力手段と、

この電話機の電話機固有データを記憶する第４の記憶手段と、

日時データを得るための時計と、

前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、

前記交換機が、

前記電話機との間で各種データの受け渡しを行う第３のデータ入出力手段と、

前記第１の記憶手段に記憶されたものと同じキーデータを記憶する第５の記憶手段と、

この第５の記憶手段に記憶されたキーデータ、及び前記第２の記憶手段に記憶され前記電話機を介して供給されるカード固有データに基づき、前記第１のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第２のカード固有キーデータ生成手段と、

この第２のカード固有キーデータ生成手段により生成されたカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、

この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、

この比較手段による比較結果から、前記電話機で取り扱われるＩＣカードの真偽を判別し、前記電話機で取り扱われるＩＣカードによる通話の可否を判定する判定手段と、

を備えたことを特徴とするＩＣカード処理システム。

【請求項２６】前記キーデータとして異なる複数のキーデータを設定し、状況に応じてこれら複数のキーデータを使い分けることを特徴とする請求項２１、請求項２２、又は請求項２５に記載のＩＣカード処理システム。

【請求項２７】前記固有キーデータ生成手段として異なる複数の固有キーデータ生成手段を設定し、状況に応じてこれら複数の固有キーデータ生成手段を使い分けることを特徴とする請求項２１、請求項２２、又は請求項２５に記載のＩＣカード処理システム。

【請求項２８】前記キーデータとして異なる複数のキーデータを設定し、かつ前記固有キーデータ生成手段として異なる複数の固有キーデータ生成手段を設定し、状況に応じてこれら複数のキーデータ及びこれら複数の固有キーデータ生成手段を使い分けることを特徴とする請求項２１、請求項２２、又は請求項２５に記載のＩＣカード処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、演算素子としてのＩＣを有するＩＣカードを処理をするＩＣカード処理システムに関する。

【０００２】

【従来の技術】現在、プリペイドカードの一種であるテレホンカードにより公衆電話が利用できるようになっている。また、将来的には、ＩＣカードにプリペイドカードとしての機能を持たせ、このＩＣカードにより公衆電話が利用できるような提案がなされている。

【０００３】上記したようにＩＣカードをプリペイドカードとして使用する場合、機器（電話機）によるカードの正当性確認（真偽判定）は、例えば、機器に固定で保持されているキー情報、又はカード使用者により入力される暗証番号の「値の照合」により行われる。

【０００４】また、より進んだ方法として、ＩＣカードが持つ乱数生成機能を利用した認証方法では、全てのカードに共通な値として格納されたキーを暗号化に使用して認証が行われる。さらに、このような認証処理が行なわれる場合、カードには一種類の暗号化キーを使用した一種類の暗号処理が適用される。

【０００５】以上説明した処理は基本的にカードを保持する機器内で、その機器が格納しているプログラム等により行なわれる。

【０００６】

【発明が解決しようとする課題】ところが、上記した従来のようなカードの正当性確認の方法では、以下のような問題があった。

【０００７】機器に固定で保持されているキー情報、又はカード使用者により入力される暗証番号等の「値の照合」によりカードの正当性を確認する場合、カードと機器の伝送内容を何らかの方法でモニターされてしまうことがある。この場合、モニターされたデータが、カード偽造・システム解析の手がかりとされてしまうことがある。

【０００８】ＩＣカードが持つ乱数生成機能を利用した認証方法では、カードと機器の間の通信で交換される乱数は都度異なる値となり、単純に内容をモニターするだけでは直接カード偽造・システム解析の手がかりとすることはできない。ところが、交わされる乱数の組を複数収集して解析することによりカード偽造・システム解析の手かがりが得られてしまうことがある。さらに、認証処理が行なわれる場合に使用される暗号化処理は一種類のため、交わされる乱数の組を複数収集して解析することによりカード偽造・システム解析の手がかりが得られてしまうことがある。

【０００９】これらの処理は基本的にカードを保持する機器内で、その機器が格納しているプログラム等により行なわれているため、機器を入手してプログラムを解析することによりカード偽造・システム解析の手がかりが得られてしまうことがある。

【００１０】この発明の目的は、上記したような事情に鑑み成されたものであって、セキュリティの要となる秘密情報が漏洩しにくいＩＣカード処理システムを提供することにある。さらに、セキュリティの要となる秘密情報が漏洩した場合でも、漏洩した秘密情報による不正使用を防止できるＩＣカード処理システムを提供することにある。

【００１１】

【課題を解決するための手段】この発明は、上記問題点に基づきなされたもので、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、外部への読み出しが禁止されたキーデータを記憶する記憶手段と、前記キーデータ及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするＩＣカードが提供される。

【００１２】また、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、プリペイドカードとしての価値を示す度数データを記憶する第１の記憶手段と、外部への読み出しが禁止されたキーデータを記憶する第２の記憶手段と、前記度数データ、キーデータ、及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするＩＣカードが提供される。

【００１３】さらに、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカード、このＩＣカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するＩＣカード処理システムにおいて、前記ＩＣカードに設けられた集積回路が、前記端末装置との間で各種データの受け渡しを行う第１のデータ入出力手段と、外部への読み出しが禁止されたキーデータを記憶する第１の記憶手段と、この第１の記憶手段に記憶されたキーデータ、及び前記端末装置から供給される端末データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、を備え、前記端末装置が、前記ＩＣカード及び前記ホスト装置との間で各種データの受け渡しを行う第２のデータ入出力手段と、この端末装置の端末固有データを記憶する第２の記憶手段と、この第２の記憶手段に記憶された端末固有データを基にして乱数データを生成する乱数データ生成手段と、を備え、前記ホスト装置が、前記端末装置との間で各種データの受け渡しを行う第３のデータ入出力手段と、前記第１の記憶手段に記憶されたものと同じキーデータを記憶する第３の記憶手段と、この第３の

記憶手段に記憶されたキーデータ及び前記端末装置から供給される乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記端末装置で取り扱われるＩＣカードの真偽を判別し、前記端末装置で取り扱われるＩＣカードによる各種処理の実行の可否を判定する判定手段と、を備えたことを特徴とするＩＣカード処理システムが提供される。

【００１４】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するＩＣカード、このＩＣカードの集積回路に記憶された度数データの度数と引き替えに通話が可能な電話機、及びこの電話機と通信対象となる他の電話機とを接続する交換機を有するＩＣカード処理システムにおいて、前記ＩＣカードに設けられた集積回路が、前記電話機との間で各種データの受け渡しを行う第１のデータ入出力手段と、前記度数データを記憶する第１の記憶手段と、外部への読み出しが禁止されたキーデータを記憶する第２の記憶手段と、前記第１の記憶手段に記憶された度数データ、前記第２の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、を備え、前記電話機が、前記ＩＣカード及び前記交換機との間で各種データの受け渡しを行う第２のデータ入出力手段と、電話機固有の電話機固有データを記憶する第３の記憶手段と、日時データを得るための時計と、前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、を備え、前記交換機が、前記電話機との間で各種データの受け渡しを行う第３のデータ入出力手段と、前記第２の記憶手段に記憶されたものと同じキーデータを記憶する第４の記憶手段と、前記第１の記憶手段に記憶され前記電話機を介して供給される度数データ、前記第４の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記電話機で取り扱われるＩＣカードの真偽を判別し、前記電話機で取り扱われるＩＣカードによる通話の可否を判定する判定手段と、を備えたことを特徴とするＩＣカード処理システムが提供される。

【００１５】またさらに、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、このＩＣカード固有のカード固有データを記憶する第１の記憶手段と、外部への読み出しが禁止されたキーデータを記憶する第２の記憶手段と、前記カード固有データ、前記キーデータ、及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするＩＣカードが提供される。

【００１６】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、プリペイドカードとしての価値を示す度数データを記憶する第１の記憶手段と、このＩＣカード固有のカード固有データを記憶する第２の記憶手段と、外部への読み出しが禁止されたキーデータを記憶する第３の記憶手段と、前記度数データ、前記カード固有データ、前記キーデータ、及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするＩＣカードが提供される。

【００１７】またさらに、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、及びこのＩＣカードを取り扱うカード処理装置を有するＩＣカード処理システムにおいて、前記発行装置が、前記ＩＣカードの集積回路に対して、ＩＣカード固有のカード固有データ及びキーデータを書き込む書込手段を備え、前記ＩＣカードに設けられた集積回路が、前記カード処理装置との間で各種データの受け渡しを行う第１のデータ入出力手段と、前記カード固有データを記憶する第１の記憶手段と、前記キーデータを外部への読み出しを禁止した状態で記憶する第２の記憶手段と、前記カード固有データ、前記キーデータ、及び前記カード処理装置から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、を備え、前記カード処理装置が、前記ＩＣカードとの間で各種データの受け渡しを行う第２のデータ入出力手段と、このカード処理装置のカード処理装置固有データを記憶する第３の記憶手段と、この第３の記憶手段に記憶されたカード処理装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、前記第２の記憶手段に記憶されたものと同じキーデータを記憶する第４の記憶手段と、前記第１の記憶手段に記憶されＩＣカードから供給されるカード固有データ、前記第４の記憶手段に記憶されたキーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、この第２

の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記ＩＣカードから供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記カード処理装置で取り扱われるＩＣカードの真偽を判別し、前記カード処理装置で取り扱われるＩＣカードによる各種処理の実行の可否を判定する判定手段と、を備えたことを特徴とするＩＣカード処理システムが提供される。

【００１８】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、このＩＣカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するＩＣカード処理システムにおいて、前記発行装置が、前記ＩＣカードの集積回路に対して、ＩＣカード固有のカード固有データ及びキーデータを書き込む書込手段を備え、前記ＩＣカードに設けられた集積回路が、前記カード処理装置との間で各種データの受け渡しを行う第１のデータ入出力手段と、前記カード固有データを記憶する第１の記憶手段と、前記キーデータを外部への読み出しを禁止した状態で記憶する第２の記憶手段と、前記カード固有データ、前記キーデータ、及び前記端末装置から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、を備え、前記端末装置が、前記ＩＣカード及び前記ホスト装置との間で各種データの受け渡しを行う第２のデータ入出力手段と、この端末装置の端末固有データを記憶する第３の記憶手段と、この第３の記憶手段に記憶された端末固有データを基にして前記乱数データを生成する乱数データ生成手段と、を備え、前記ホスト装置が、前記端末装置との間で各種データの受け渡しを行う第３のデータ入出力手段と、前記第２の記憶手段に記憶されたものと同じキーデータを記憶する第４の記憶手段と、前記第１の記憶手段に記憶されＩＣカードから供給されるカード固有データ、前記第４の記憶手段に記憶されたキーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記端末装置で取り扱われるＩＣカードの真偽を判別し、前記端末装置で取り扱われるＩＣカードによる各種処理の実行の可否を判定する判定手段と、を備えたことを特徴とするＩＣカード処理システムが提供される。

【００１９】またさらに、この発明によれば、各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、このＩＣカードの集積回路に記憶された度数データの度数と引き替えに通話が可能な電話機、及びこの電話機と通信対象となる他の電話機とを接続する交換機を有するＩＣカード処理システムにおいて、前記発行装置が、前記ＩＣカードの集積回路に対して、ＩＣカード固有のカード固有データ、度数データ、及びキーデータを書き込む書込手段を備え、前記ＩＣカードに設けられた集積回路が、前記電話機との間で各種データの受け渡しを行う第１のデータ入出力手段と、前記カード固有データを記憶する第１の記憶手段と、前記度数データを記憶する第２の記憶手段と、前記キーデータを外部への読み出しを禁止した状態で記憶する第３の記憶手段と、前記第１の記憶手段に記憶されたカード固有データ、前記第２の記憶手段に記憶された度数データ、前記第３の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、を備え、前記電話機が、前記ＩＣカード及び前記交換機との間で各種データの受け渡しを行う第２のデータ入出力手段と、電話機固有の電話機固有データを記憶する第４の記憶手段と、日時データを得るための時計と、前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、を備え、前記交換機が、前記電話機との間で各種データの受け渡しを行う第３のデータ入出力手段と、前記第３の記憶手段に記憶されたものと同じキーデータを記憶する第５の記憶手段と、前記第１の記憶手段に記憶され前記電話機を介して供給されるカード固有データ、前記第２の記憶手段に記憶され前記電話機を介して供給される度数データ、前記第５の記憶手段に記憶されたキーデータ、及び前記電話機から供給される乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記電話機で取り扱われるＩＣカードの真偽を判別し、前記電話機で取り扱われるＩＣカードによる通話の可否を判定する判定手段と、を備えたことを特徴とするＩＣカード処理システムが提供される。

【００２０】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、このＩＣカード固有のカード固有データを記憶する第１の記憶手段と、外部への読み出しが禁止されたものであって、前記カード固有データから生成されるカード固有のカード固有キーデータを記憶する第２の記憶手段と、前記カード固有キーデータ及び外部から供給される外部データを基にして、このＩＣ

カードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするＩＣカードが提供される。

【００２１】またさらに、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカードにおいて、この集積回路が、外部との間で各種データの受け渡しを行うデータ入出力手段と、プリペイドカードとしての価値を示す度数データを記憶する第１の記憶手段と、このＩＣカード固有のカード固有データを記憶する第２の記憶手段と、外部への読み出しが禁止されたものであって、前記カード固有データから生成されるカード固有のカード固有キーデータを記憶する第３の記憶手段と、前記度数データ、カード固有キーデータ、及び外部から供給される外部データを基にして、このＩＣカードを認証するための認証データを生成する認証データ生成手段と、を備えたことを特徴とするＩＣカードが提供される。

【００２２】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、及びこのＩＣカードを取り扱うカード処理装置を有するＩＣカード処理システムにおいて、前記発行装置が、キーデータを記憶する第１の記憶手段と、前記キーデータ及びＩＣカードに対して付与されるＩＣカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第１のカード固有キーデータ生成手段と、前記ＩＣカードの集積回路に対して、前記カード固有データ及び前記カード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、前記ＩＣカードに設けられた集積回路が、前記カード処理装置との間で各種データの受け渡しを行う第１のデータ入出力手段と、前記カード固有データを記憶する第２の記憶手段と、前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第３の記憶手段と、前記カード固有キーデータ及び前記カード処理装置から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、を備え、前記カード処理装置が、前記ＩＣカードとの間で各種データの受け渡しを行う第２のデータ入出力手段と、このカード処理装置のカード処理装置固有データを記憶する第４の記憶手段と、この第４の記憶手段に記憶されたカード処理装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、前記第１の記憶手段に記憶されたものと同じキーデータを記憶する第５の記憶手段と、この第５の記憶手段に記憶されたキーデータ、及び前記第２の記憶手段に記憶され前記ＩＣカードを介して供給されるカード固有データに基づき、前記第１のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第２のカード固有キーデータ生成手段と、前記第２のカード固有キーデータ生成手段により生成されるカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記ＩＣカードから供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記カード処理装置で取り扱われるＩＣカードの真偽を判別し、前記カード処理装置で取り扱われるＩＣカードによる各種処理の実行の可否を判定する判定手段と、を備えたことを特徴とするＩＣカード処理システムが提供される。

【００２３】またさらに、この発明によれば、各種演算処理を実行する集積回路を有するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、このＩＣカードを取り扱う端末装置、及びこの端末装置を監視するホスト装置を有するＩＣカード処理システムにおいて、前記発行装置が、キーデータを記憶する第１の記憶手段と、前記キーデータ及びＩＣカードに対して付与されるＩＣカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第１のカード固有キーデータ生成手段と、前記ＩＣカードの集積回路に対して、前記カード固有データ及び前記第１のカード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、前記ＩＣカードに設けられた集積回路が、前記端末装置との間で各種データの受け渡しを行う第１のデータ入出力手段と、前記カード固有データを記憶する第２の記憶手段と、前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第３の記憶手段と、前記カード固有キーデータ及び前記端末装置から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、を備え、前記端末装置が、前記ＩＣカードとの間で各種データの受け渡しを行う第２のデータ入出力手段と、この端末装置の端末固有データを記憶する第４の記憶手段と、この第４の記憶手段に記憶された端末装置固有データを基にして前記乱数データを生成する乱数データ生成手段と、前記ホスト装置が、前記端末装置との間で各種データの受け渡しを行う第３のデータ入出力手段と、前記第１の記憶手段に記憶されたものと同じキーデータを記憶する第５の記憶手段と、この第５の記憶手段に記憶されたキーデータ、及び前記第２の記憶手段に記憶され前記ＩＣカードを介して供給されるカード固有データに基づき、前記第１のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第２のカード固有キーデータ生成手段と、前記第２のカード固有キーデータ生成手段により生成されたカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第１の認証データ生成手段と同様にして認証デ

ータを生成する第２の認証データ生成手段と、この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記端末装置を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記端末装置で取り扱われるＩＣカードの真偽を判別し、前記端末装置で取り扱われるＩＣカードによる各種処理の実行の可否を判定する判定手段と、を備えたことを特徴とするＩＣカード処理システムが提供される。

【００２４】さらにまた、この発明によれば、各種演算処理を実行する集積回路を有しこの集積回路に記憶される度数データによりプリペイドカードとして機能するＩＣカードを発行する発行装置、この発行装置により発行されるＩＣカード、このＩＣカードの集積回路に記憶された度数データの度数と引き替えに通話が可能な電話機、及びこの電話機と通信対象となる他の電話機とを接続する交換機を有するＩＣカード処理システムにおいて、前記発行装置が、キーデータを記憶する第１の記憶手段と、前記キーデータ及びＩＣカードに対して付与されるＩＣカード固有のカード固有データに基づき、カード固有のカード固有キーデータを生成する第１のカード固有キーデータ生成手段と、前記ＩＣカードの集積回路に対して、前記カード固有データ及び前記第１のカード固有キーデータ生成手段により生成されたカード固有キーデータを書き込む書込手段を備え、前記ＩＣカードに設けられた集積回路が、前記電話機との間で各種データの受け渡しを行う第１のデータ入出力手段と、前記カード固有データを記憶する第２の記憶手段と、前記カード固有キーデータを外部への読み出しを禁止した状態で記憶する第３の記憶手段と、前記カード固有キーデータ及び前記電話機から供給される乱数データを基にして、このＩＣカードを認証するための認証データを生成する第１の認証データ生成手段と、を備え、前記電話機が、前記ＩＣカードとの間で各種データの受け渡しを行う第２のデータ入出力手段と、この電話機の電話機固有データを記憶する第４の記憶手段と、日時データを得るための時計と、前記電話機固有データ及び前記日時データを基にして前記乱数データを生成する乱数データ生成手段と、前記交換機が、前記電話機との間で各種データの受け渡しを行う第３のデータ入出力手段と、前記第１の記憶手段に記憶されたものと同じキーデータを記憶する第５の記憶手段と、この第５の記憶手段に記憶されたキーデータ、及び前記第２の記憶手段に記憶され前記電話機を介して供給されるカード固有データに基づき、前記第１のカード固有キーデータ生成手段と同様にしてカード固有キーデータを生成する第２のカード固有キーデータ生成手段と、この第２のカード固有キーデータ生成手段により生成されたカード固有キーデータ、及び前記乱数生成手段により生成された乱数データを基にして、前記第１の認証データ生成手段と同様にして認証データを生成する第２の認証データ生成手段と、この第２の認証データ生成手段で生成された認証データと、前記第１の認証データ生成手段で生成され前記電話機を介して供給される認証データとを比較する比較手段と、この比較手段による比較結果から、前記電話機で取り扱われるＩＣカードの真偽を判別し、前記電話機で取り扱われるＩＣカードによる通話の可否を判定する判定手段と、を備えたことを特徴とするＩＣカード処理システムが提供される。

【００２５】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照して説明する。

【００２６】図１～図１２は、この発明の一形態に係るＩＣカード処理システムを構成するＩＣカード、ＩＣカード発行機、ＩＣカードを直接取り扱う端末装置としての電話機、及び電話機と電話機とを取り繋ぐ交換機を説明するための図である。なお、この実施の形態では、プリペイドカードとしての価値を示す度数データをＩＣカードに記録して、このＩＣカードに記録された度数と引き替えに電話機が利用できるような公衆電話のシステムに適用した場合について説明する。

【００２７】まず、図１を参照して、ＩＣカードについて簡単に説明する。図１は、ＩＣカードの外観を示す概略図である。この発明のＩＣカード処理システムで使用されるＩＣカード３００には、図１に示すように、磁気ストライプ３０２及びＩＣモジュール３０４などが設けられている。また、このＩＣカード３００は、ＩＳＯ等の規格に基づき形成されるものとする。

【００２８】ここで、ＩＣモジュール３０４について簡単に説明しておく。ＩＣモジュール３０４には、例えばＰ１～Ｐ８の８本の端子（ピン）が設けられている。Ｐ１は、後述するカードリーダ・ライタからの動作電流をカードに供給する端子である。Ｐ２は、カードリーダ・ライタからのリセット信号をカードに供給するピンである。Ｐ３は、カードリーダ・ライタからの動作用クロックを供給する端子である。Ｐ５は、グランド端子である。Ｐ７は、カードリーダ・ライタからの書込電圧を供給する端子である。Ｐ８は、双方向のシリアルなデータ伝送路として機能する端子である。

【００２９】続いて、図２を参照して、ＩＣカード３００の製造手順について説明する。図２は、ＩＣカードの製造手順を示すフローチャートである。

【００３０】ＩＣカード３００のＩＣモジュール３０４の原型であるＩＣチップ３０５は、図３に示すように、演算素子としてのＣＰＵ３１０、及びＲＯＭ３３１並びにＲＡＭ３３２を含むメモリ３３０等で構成されている。このメモリ３３０には、ＣＰＵ３１０を制御するカード制御プログラムが記憶される。

【００３１】ＩＣカード製造行程の始めの段階では、後述する認証子を生成するための認証子生成関数を含む前

記カード制御プログラム（マスクプログラム）が作成される（ＳＴ２）。このカード制御プログラムは、ＩＣチップ３０５のメモリ３３０にに登録される（ＳＴ４）。カード制御プログラムが登録されたＩＣチップ３０５はモジュール化され（ＳＴ６）、モジュール化されたＩＣモジュール３０４はＩＣカード３００に埋め込まれる（ＳＴ８）。このようにしてＩＣカードが製造される。

【００３２】続いて、図４を参照して、ＩＣカードを発行する発行機２００について説明する。図４は、発行機２００の外観を示す概略図である。

【００３３】図４に示すように、発行機２００は、ＩＣカードに対してデータを書き込んだりＩＣカードに書き込まれたデータを読み出したりするＩＣカードリーダ・ライタ２２０、及びこのカードリーダ・ライタ２２０を制御するパーソナルコンピュータ（ＰＣ）２０１等により構成されている。

【００３４】なお、以下説明する発行機２００の機能は、このＰＣ２０１を制御する発行機ＣＰＵ２１０の制御プログラムにより実現されるものとする。勿論、これは最低限の構成であり、ＩＣカードを多数枚発行する必要がある場合には、自動的にＩＣカードを取り込み／送り出して複数枚を連続して自動発行する仕様が必要となる。

【００３５】続いて、図５を参照して、発行機２００によるＩＣカードの発行の流れについて説明する。図５は、発行機２００によるＩＣカードの発行を説明するフローチャートである。

【００３６】まず、ＰＣ２０１上でのデータの入力編集作業として後述する認証子を生成するための認証子生成用秘密鍵が設定される（ＳＴ１１）。認証子生成用秘密鍵は、例えば、ＰＣ２０１のキーボードから入力したり、認証子生成用秘密鍵が記録されたディスクから読み取ったりして設定される。また、システムとして認証子生成用秘密鍵が使用される場合には、予めＰＣ２０１の発行機ＣＰＵ２３０の制御プログラムコードに含ませるようにしてもよい。あるいは、このとき使用されていないカードリーダ・ライタ２２０を使用して、システムとして用意された設定用ＩＣカードから読みとるようにしてもよい。

【００３７】次に、ＰＣ２０１の操作により、これから発行するＩＣカードへ設定するための度数（５０度数、１００度数等）が選択される（ＳＴ１２）。多数枚のＩＣカードを連続発行する場合、度数ごとに複数組の発行機２００を用意し各発行機ごとに扱う度数を固定するようにしてもよい。

【００３８】上記したように認証子生成用秘密鍵が設定され度数が選択されるとカード発行準備が整い、カードリーダ・ライタ２２０でＩＣカード挿入待ちとなる。カードリーダ・ライタ２２０にＩＣカードが挿入されると（ＳＴ１３）、ＩＣカードに対して前記設定された認証子生成用秘密鍵及び前記選択された度数が書き込まれる（ＳＴ１４）。多数枚のＩＣカードを連続発行する場合、未発行カードをまとめてスタックしておき自動的に一枚抜き取って書き込み位置まで搬送するような自動取り込み方式をとるようにしてもよい。

【００３９】その後、カードリーダ・ライタ２２０からＩＣカードが抜き取られ（ＳＴ１５）、一枚のＩＣカードの発行操作が完了する。多数枚のＩＣカードを連続発行する機器の場合、発行済みＩＣカードを自動的に搬送して機器外へ送り出したり、機器内外の発行済みＩＣカード収納部へ搬送して積み重ねる形で格納するような自動搬送方式をとるようにしてもよい。ＳＴ１３～ＳＴ１５の繰り返しにより、次々とＩＣカードが発行されることになる（ＳＴ１６）。

【００４０】ここで、図６～図８を参照して、設定用ＩＣカードについて説明する。設定用ＩＣカードとは、上記したようにＩＣカード処理システムにおいて必要とされるデータ、例えば認証子生成用秘密鍵のようなものをシステムに設定するために使用されるものである。このような設定用ＩＣカードを利用することにより、機密データを安全にシステムに設定することができる。勿論、この設定用ＩＣカードに記録されているデータは容易に外部に読み出せないようになっている。

【００４１】ここで、設定用ＩＣカードから認証子生成用秘密鍵を発行機２００に設定するケースについて説明する。設定用ＩＣカードから認証子生成用秘密鍵を読み出すにあたっては、ＰＣ２０１即ち発行機２００と設定用ＩＣカードとの間で何らかの正当性確認をする運用が必要となる。

【００４２】単純には、発行機２００側のプログラムの一部として格納されているキー情報をカードへ送り、カード内で照合してキー情報の正当性が確認されてから認証子生成用秘密鍵を読み出すことができる様にする（図６）。これにより、タイプミス等による誤った値の認証子生成用秘密鍵の登録が回避されるだけでなく、認証子生成用秘密鍵はＩＣカード３００と発行機２００の間の通信データとして出現するだけとなり、外部への漏洩の機会が減少する。

【００４３】また、認証子生成用秘密鍵の暗号化については、設定用ＩＣカードに暗号化機能を持たせ、生データとして記憶している認証子生成用秘密鍵を送出時に暗号化する方法（図７）や、設定用ＩＣカードへ既に暗号化済みの認証子生成用秘密鍵を記憶させておきそのまま送出させる方法（図８）等が考えられる。

【００４４】また、この様な設定用ＩＣカードを作成する機能を、発行機２００に併せ持たせる方法と、別システムとして用意する方法とが考えられる。さらに、発行機２００と設定用ＩＣカードの間の正当性確認に相互認証を使用することによって、発行機２００側として偽の設定用ＩＣカードにより偽の認証子生成用秘密鍵を設定

されることによる業務妨害が回避できる。これは、第三者が悪意で設定用ＩＣカードをすり替えることによって、誤った認証子生成用秘密鍵が設定された正常に使用できないカードを市中に出回らせ、カード及びシステムの信頼性を失墜させる様な妨害に利用される。すなわち、システム全体の解析により電話がかけられるカードを偽造することは困難だが、設定用ＩＣカードに相互認証を適用していなければ、発行機２００からのキー照合に際していかなるキー値に対しても正当であると応え、偽の認証子生成用秘密鍵を送出する為の設定用ＩＣカードは、幾分偽造しやすいためである。

【００４５】ここで、図９を参照して上記した相互認証の手順について説明する。図９は、相互認証を説明する図である。ここでは、上位機器ＸとＩＣカードＹとの相互認証を例にとり説明する。

【００４６】第１に、内部認証（上位機器Ｘ側での認証処理）について説明する。まず、上位機器Ｘ側で、乱数Ｒ１が生成される（ＳＴ２０）。この生成された乱数Ｒ１がＩＣカードＹへ送られる（ＳＴ２２）。ＩＣカードＹ側において、乱数Ｒ１が予め設定された内部認証用キーＫ１により暗号化され、暗号化キーＲ２Ｙが生成される（ＳＴ２４）。この生成された暗号化キーＲ２Ｙは、ＩＣカードＹ側から上位機器Ｘ側へ送信される（ＳＴ２６）。

【００４７】一方、上位機器Ｘ側では、乱数Ｒ１が予め設定された内部認証用キーＫ１により暗号化され、暗号化キーＲ２Ｘが生成される（ＳＴ２８）。この生成された暗号化キーＲ２Ｘと、ＩＣカードＹ側で生成され送られてきた暗号化キーＲ２Ｙとが比較され（ＳＴ３０）、この比較結果により上位機器Ｘ側において、ＩＣカードＹの真偽が判定される（ＳＴ３２）。即ち、暗号化キーＲ２Ｘ＝Ｒ２Ｙとなれば、ＩＣカードＹは真と判定される（以上内部認証）。

【００４８】第２に、外部認証（ＩＣカードＹ側での認証処理）について説明する。まず、上位機器Ｘ側からＩＣカードＹに対して、外部認証の要求が出される（ＳＴ３４）。この要求に従い、ＩＣカードＹ側において、乱数Ｒ３が生成される（ＳＴ３６）。この生成された乱数Ｒ３が、上位機器Ｘへ送られる（ＳＴ３８）。上位機器Ｘ側において、乱数Ｒ３が予め設定された外部認証用キーＫ２により暗号化され、暗号化キーＲ４Ｘが生成される（ＳＴ４０）。この生成された暗号化キーＲ４Ｘは、上位機器Ｘ側からＩＣカードＹ側へ送信される（ＳＴ４２）。

【００４９】一方、ＩＣカードＹ側では、乱数Ｒ３が予め設定された内部認証用キーＫ２により暗号化され、暗号化キーＲ４Ｙが生成される（ＳＴ４４）。この生成された暗号化キーＲ４Ｙと、上位機器Ｘ側で生成され送られてきた暗号化キーＲ４Ｘとが比較され（ＳＴ４６）、この比較結果によりＩＣカードＹ側において、上位機器Ｘの真偽が判定される（ＳＴ４８）。即ち、暗号化キーＲ４Ｘ＝Ｒ４Ｙとなれば、上位機器Ｘは真と判定される（以上内部認証）。上位機器Ｘが真と判定されると、このＩＣカードＹからのデータの読み出しが許可され、比較結果がレスポンスとして上位機器Ｘに送信される（ＳＴ５０）。

【００５０】続いて、図１０を参照して、電話機４００について説明する。図１０は、電話機４００の外観を示す概略図である。

【００５１】図１０に示すように、電話機４００は、送受話器４０１、プッシュ式ボタン４０２、ＩＣカード３００の挿入を受け付けるとともにＩＣカード３００を返却するカード挿入口４０３、及びＩＣカード３００に記録された度数データの残りを表示する表示部４０４などで構成されている。

【００５２】ここで、図１１を参照して、電話機４００の製造手順について説明する。図１１は、電話機４００の製造手順を示すフローチャートである。

【００５３】考え方はＩＣカード３００の製造の場合と似ており、基本的な構成のハードウェア及びこのハードを制御するソフトウェアに対して、この実施形態で適用する特別な機能を実現するためのハードとソフトを追加する事になる。

【００５４】まず、ハードウェア製造時において、後述する乱数生成時における乱数生成の種の一つとなる日時データを取得するための時計回路が搭載される（ＳＴ６０）。

【００５５】次に、認証子を生成するために必要な乱数を生成する乱数生成プログラム、カードのアクセスプログラム、及び交換機５００との間で種々のやりとりをするプログラムを、基本的な電話機制御を司る電話機制御プログラムに包含して作成する（ＳＴ６２）。

【００５６】このようにして作成された電話機制御プログラムを、先にハードウェアだけ製造済みの電話機４００に搭載する。この方法としては、例えば別工程でこの電話制御プログラムが書き込まれたＲＯＭを、電話機４００の制御基板上のＲＯＭソケットに差し込むことで行なったり、制御基板上にあるいは機体内のメモリカード等の不揮発性あるいはバッテリバックアップされたメモリに通信等で書き込むことで行なったり、あるいは電話機４００にディスク装置を内蔵する様な場合にはこれに書き込むことで行なったりしてもよい（ＳＴ６４）。

【００５７】さらに、後述する乱数生成時に乱数生成のもう一つの種となる各電話機毎に固有の電話機番号（機体個別番号）を電話機に登録する必要がある。この実施形態では、前記の様な方法でプログラム登録が完了した電話機４００のボタン４０２により電話機番号を入力し登録する（ＳＴ６６）。

【００５８】ここで、電話機番号の登録の一例について簡単に説明する。前記したように制御プログラムの登録

が完了した電話機４００に対してはじめて電源が投入されると、電話機番号が登録されていないので電話機番号が入力されるのを待つ状態となる。すなわち、電話機のプログラムは起動の都度電話機番号の登録状態を検査し登録されていない場合、電話機番号入力待ち状態となる。このとき、カード残度数表示部４０４には、「－－－」が表示されるので、ボタン４０２から電話機番号が入力されることになる。まず、最初に押下されたボタン４０２に対応した数字が表示部４０４の右側に表示され、「－－Ａ」（Ａは押下されたボタンに対応した数字）となる。さらに、ボタン４０２が押下されると「－ＡＢ」（Ｂは次に押下されたボタンに対応した数字）、またさらに、ボタン４０２が押下されると「ＡＢＣ」（Ｃはまた次に押下されたボタンに対応した数字）、さらにまた、ボタン４０２が押下されると「ＢＣＤ」（Ｄはそのまた次に押下されたボタンに対応した数字）という様に順送り表示される。最終桁までの入力が完了したら「＊」を押すと表示が点滅して確認待ちとなり「＃」を押すことで入力された電話機番号が決定され電話機内部のＲＯＭに書き込まれる。一旦電話機番号が登録された後は、カード式電話機としての標準的動作に移る。

【００５９】一旦電源が断たれ、再度通電して再起動した際に電話機のプログラムは電話機番号の登録状態を検査し、それが登録済みであることを確認して電話機番号登録動作をスキップしてカード式電話機としての標準的動作に移る。

【００６０】上記したようにボタン４０２と表示部４０４を使う方法の他、送受話器４０１で音声入力したり、通信で登録したり、前記プログラム登録時にプログラムの一部として登録する等のようにしてもよい。

【００６１】この様な工程を経て完成した電話機４００は公衆電話として市中の各所に設置されることになる。

【００６２】続いて、図１２参照して交換機５００について説明する。図１２は、交換機５００の外観を示す概略図である。

【００６３】図１２に示すように、交換機５００は、交換機本体５０１、及びこの交換機本体５０１に対して各種指示を行うパーソナルコンピュータ（ＰＣ）５０２などで構成されている。

【００６４】ここで、図１３を参照して、交換機５００の製造手順について説明する。図１３は、交換機５００の製造手順を示すフローチャートである。

【００６５】考え方は電話機４００と同様であり、基本的な構成のハードウェアとそれを制御するソフトウェアに対してこの実施形態で適用する特別な機能を実現するためのハードとソフトを追加する事になる。

【００６６】まずハードウェア製造時において、電話機４００と通信を行うインターフェイスが搭載される（ＳＴ７０）。

【００６７】次に、ＩＣカード３００に登録されるのと同じ認証子生成用秘密鍵、同じ認証子生成関数、及び電話機とＩＣカード３００との間で種々のやりとりをするプログラムを、基本的な交換機制御を司る交換機制御プログラムに包含して作成する（ＳＴ７２）。

【００６８】このようにして作成された交換機制御プログラムを、先にハードウェアだけ製造済みの交換機本体５０１に搭載する。この方法としては、例えば別工程でこの交換機制御プログラムが書き込まれたＲＯＭを、交換機の制御基板上のＲＯＭソケットに差し込むことで行なったり、制御基板上にあるいは機体内のメモリカード等の不揮発性あるいはバッテリバックアップされたメモリに通信等で書き込むことで行なったり、あるいは交換機本体５０１にディスク装置を内蔵する様な場合にはこれに書き込むことで行なったりしてもよい（ＳＴ７４）。

【００６９】この様な工程を経て完成した交換機５００はしかるべき管理者以外は触れられないセキュリティの確保された環境に設置される。

【００７０】なお、ＩＣカード３００に格納される認証子生成用秘密鍵、プリペイドの度数、認証子生成関数のプログラムの各情報の格納タイミングの上記以外のバリエーションに限定されるものではない。例えば、認証子生成関数のプログラムだけでなく、販売額に当たる基本度数をＩＣカードの基本プログラム（ＯＳ）の一部として製造時に登録しておき、それ以外のデータ部分について発行機で書き込むパターン（この場合の残度数は当初の基本度数をもとに計算する）や、完全なユニーク性を確保するためにはカード個別番号だけをＯＳ内に固定データとして製造時に登録し、それ以外を発行機で書き込むパターン等が考えられる。これ以外にも種々のパターンがあるので、全ての組み合わせについてそれ以降の本発明で示す処理に適用できるため、ここに示した以外の格納タイミングのパターンを排除するものではない。

【００７１】次に、この発明のポイントであるＩＣカード処理システムにおけるセキュリティについて第１の実施形態～第３の実施形態に分けて説明する。

【００７２】最初に、図１４を参照して第１の実施形態について説明する。図１４は、この発明の第１の実施形態に係るＩＣカード処理システムを示す図である。

【００７３】まず、製造設備１００によりＩＣカード３００が製造される。このＩＣカード製造行程では、認証子生成関数を含むマスクプログラムが作成され、この認証子生成関数を含むマスクプログラムがＩＣチップ３０５のメモリ３３０に登録される。さらにこのＩＣチップ３０５がモジュール化され、このモジュール化されたＩＣモジュール３０４が、ＩＣカードへ埋め込まれＩＣカード３００が製造される。つまり、このＩＣカード製造行程において、ＩＣカード３００のメモリ３３０に対して認証子生成関数が登録されたことになる。

【００７４】次に、上記のような製造行程を経て製造さ

れたＩＣカード３００に対して、発行機２０による発行処理がなされる。この発行機２００は、発行機ＣＰＵ２１０により制御されており、この発行機ＣＰＵ２１０を制御する発行機制御プログラム及びＩＣカードに渡す度数情報等はメモリ２３０に記憶されている。また、この実施形態では、発行機制御プログラムに、認証子生成用秘密鍵が含まれているものとする。このような発行機２００のカードリーダ・ライタ２２０により、ＩＣカード３００に対して度数情報及び認証子生成用秘密鍵が登録される。

【００７５】次に、上記製造工程及び発行処理を経たＩＣカード３００について説明する。このＩＣカード３００は、ＩＣカードＣＰＵ３１０により制御されており、このＩＣカードＣＰＵ３１０を制御するカード制御プログラム及び発行機２００から送られる度数情報並びに認証子生成用秘密鍵等はメモリ３３０に記憶されている。また、この時点で、カード制御プログラムには、認証子生成関数が含まれている。さらに、このＩＣカード３００は、電話機４００との間で各種データの受け渡しを行うインターフェース３２０を備えている。

【００７６】次に、ＩＣカード３００を取り扱う端末装置としての電話機４００について説明する。この電話機４００は、前記説明したような製造行程を経て製造される。つまり、電話機４００は、電話機ＣＰＵ４１０により制御されており、この電話機ＣＰＵ４１０を制御する電話機制御プログラム及び前記した電話機番号等はメモリ４３０に記憶されている。また、この実施形態では、電話機制御プログラムに、乱数生成関数が含まれているものとする。さらに、この電話機４００には、時計回路４４０が搭載され、この時計回路４４０から日時情報が取得される。そして、この時計回路４１０から得られる日時情報及びメモり４３０に記憶されている電話機番号を基にして、メモリ４３０に記憶された電話機制御プログラムに含まれる乱数生成関数により乱数が生成される。さらに、この電話機４００は、交換機５００との間で各種データの受け渡しを行うインターフェース４２０を備えている。

【００７７】次に、電話機と電話機とを接続する交換機５００について説明する。交換機５００は、前記説明したような製造行程を経て製造される。つまり、交換機５００は、交換機ＣＰＵ５１０により制御されており、この交換機ＣＰＵ５１０を制御する制御プログラム及びＩＣカード３００のメモリ３３０に記憶された認証子生成用秘密鍵と同じ認証子生成用秘密鍵等はメモリ５３０に記憶されている。また、この実施形態では、交換機制御プログラムに、カード制御プログラムに含まれた認証子生成関数と同じ認証子生成関数等が含まれているものとする。さらに、この交換機５００には、メモリ５３０内の認証子生成関数により生成された認証子と、ＩＣカード３００のメモリ３３０内の認証子生成関数により生成された認証子とを比較する比較部５４０、及びこの比較部５４０の比較結果からＩＣカード３００による通話の可否を判定する判定部５５０を備えている。さらに、この交換機５００は、電話機４００との間で各種データの受け渡しを行うインターフェース５２０を備えている。

【００７８】上記説明したような発行機２００、ＩＣカード３００、電話機４００、及び交換機５００を有するＩＣカード処理システムにおけるセキュリティは次のようにして守られる。

【００７９】例えば、電話機４００にＩＣカード３００が差し込まれると、電話機４００はメモリ４３０内の乱数生成関数を使用して、メモリ４３０内の電話機番号と時計回路４４０から取得される日時データから乱数を生成しカードへ送る。因みに、時計回路４４０から取得される日時情報は取得の都度異なる値となるため、乱数も都度異なる値として生成される。

【００８０】電話機４００で生成された乱数を受け取ったカード３００側では、メモリ３３０内の認証子生成関数を使用して、電話機で生成された乱数、メモリ３３０内の秘密鍵及び度数情報から認証子を生成する。生成された認証子は、メモリ３３０内の度数情報とともに電話機４００へ送られる。

【００８１】ＩＣカード３００からの度数情報及び認証子を受け取った電話機４００は、これら度数情報及び認証子を、先に生成しＩＣカード３００へ送った乱数とともに交換機５００へ送る。

【００８２】この交換機５００は、電話局や交換センター等に設置される、回線交換設備又は施設といったイメージのものである。交換機５００は、メモリ５３０内の認証子生成関数と秘密鍵を使用して、電話機４００から送られた度数情報及び乱数から交換機独自に認証子を生成する。さらに、交換機５００は、比較部５４０において交換機５００自身で生成された認証子と、電話機４００経由で送られてきた認証子とを比較する。そして、通話可否判定部５５０において、比較結果から電話機４００に差し込まれたＩＣカードによる通話の可否判定が下される。例えば、自身で生成された認証子と電話機４００経由で送られてきた認証子とが一致すれば、電話機４００に差し込まれたＩＣカードによる通話が許可され、回線が接続される。

【００８３】続いて、図１５を参照して第２の実施形態について説明する。図１５は、この発明の第２の実施形態に係るＩＣカード処理システムを示す図である。

【００８４】この第２の実施形態では、第１の実施形態で説明したセキュリティをより強固なものとするため、認証子生成の種として全てのＩＣカード３００に対して異なる値をとるカード個別番号（各ＩＣカードに固有の番号）を利用する。このカード個別番号は、発行機２００による発行処理の際にＩＣカード３００に対して付与されるものであり、ＩＣカード３００のメモリ３３０に

記憶される。

【００８５】すなわちＩＣカードの製造または発行時に、全てのＩＣカードに対して全て異なる値をとるカード個別番号を設定し、ＩＣカード３００内及び交換機５００での認証子生成に利用する。そのためには、電話機４００に差し込まれたＩＣカード３００のカード個別番号を交換機５００へ送る必要がある。カード個別番号は、前記説明した第１の実施形態において度数情報等を交換機５００へ送るのと同様にして交換機５００へ送られる。これによりＩＣカードから出力され電話回線経由で伝えられる認証子をより複雑化することができる。

【００８６】さらに、この第２の実施形態では、第１の実施形態で説明したセキュリティをより強固なものとするため、ＩＣカード３００と交換機５００相互に同じ値を持ち合う秘密鍵を複数組用意し、必要に応じて適用する秘密鍵を変更する。これら複数組の秘密鍵は、第１の実施形態と同様に、ＩＣカード３００のメモリ３２０、交換機５００のメモリ５３０に記憶される。勿論、ＩＣカード３００のメモリ３２０に記憶される複数組の秘密鍵と、交換機５００のメモリ５３０に記憶される複数組の秘密鍵とは同じものである。

【００８７】例えばＩＣカード３００には、発行時にＫ１、Ｋ２、…、Ｋｎ、…、ＫＮの複数種の秘密鍵を格納しておき、当初はカード、交換機ともＫａ（１≦ａ≦Ｎ）で前記第１の実施形態の運用を開始する。ある一定期間を経過したりその時使用している秘密鍵が漏洩した懸念が発生した場合、ＩＣカードが差し込まれた際に、電話機４００経由で交換機５００からＩＣカード３００へ、今後はＫｂ（１≦ｂ≦Ｎ、ｂ≠ａ）を適用するよう設定する命令を送り、同時に交換機５００側も処理にＫｂを適用する。この設定されたＩＣカード３００は、その後は交換機から指示がなくてもＫｂを処理に適用する。

【００８８】また、交換機側５００での秘密鍵管理はＩＣカード３００に格納されているＫ１～ＫＮ全てを当初から制御プログラムに包含しておき、そのいずれを適用するかを選択する方法と、常に１種類だけ保持し都度入れ替え（書き換え）る方式が考えられる。これにより、秘密鍵の解析がより困難になる。

【００８９】但し、適用する鍵を変更する命令を永続的にカードに送り続けることは、システムの解析を容易にするため、鍵変更の命令を送るのは一定期間だけ（半年間程度）とし、その期間に使用されなかった（電話機４００に差し込まれなかった）ＩＣカード３００については、窓口等に持ってきてもらう運用により不正カードを除去できる。

【００９０】このような第２の実施形態のＩＣカード処理システムにおけるセキュリティは次のようにして守られる。

【００９１】まず、製造設備１００で認証子生成関数を含むカード制御プログラムがＩＣカード３００へ登録される。さらに、発行機２００でカード個別番号、度数、及び秘密鍵１～Ｎがカードへ登録される。この秘密鍵は何らかの手法で予め決定されている値である。

【００９２】例えば、電話機４００にＩＣカード３００が差し込まれると、電話機４００はメモリ４３０内の乱数生成関数を使用して、メモリ４３０内の電話機番号と時計回路４４０から取得される日時データから乱数を生成しカードへ送る。因みに、時計回路４４０から取得される日時情報は取得の都度異なる値となるため、乱数も都度異なる値として生成される。

【００９３】電話機４００で生成された乱数を受け取ったカード３００側では、メモリ３３０内の認証子生成関数を使用して、電話機で生成された乱数、メモリ３３０内の秘密鍵とカード個別番号、及び度数情報から認証子を生成する。生成された認証子は、メモリ３３０内の度数情報及びカード個別番号とともに電話機４００へ送られる。

【００９４】ＩＣカード３００からの度数情報、カード個別番号、及び認証子を受け取った電話機４００は、これら度数情報、カード個別番号、及び認証子を、先に生成しＩＣカード３００へ送った乱数とともに交換機５００へ送る。

【００９５】交換機５００は、メモリ５３０内の認証子生成関数と秘密鍵を使用して、電話機４００から送られた度数情報、カード個別番号、及び乱数から交換機独自に認証子を生成する。さらに、交換機５００は、比較部５４０において交換機５００自身で生成された認証子と、電話機４００経由で送られてきた認証子とを比較する。そして、通話可否判定部５５０において、比較結果から電話機４００に差し込まれたＩＣカードによる通話の可否判定が下される。例えば、自身で生成された認証子と電話機４００経由で送られてきた認証子とが一致すれば、電話機４００に差し込まれたＩＣカードによる通話が許可され、回線が接続される。

【００９６】ある秘密鍵による運用が一定期間継続した場合や、秘密鍵漏洩の懸念が発生した場合、交換機５００から電話機４００経由で秘密鍵変更コマンドが送られ、以降運用に適用される秘密鍵が変更される。

【００９７】なお、第２の実施形態で使用するカード個別番号のカードへの登録設定は、第１の実施形態を実現する各機器の中ではＩＣカード３００自体の製造時に登録してしまうか、或いは上記したように発行機２００で書き込む方法が考えられる。発行機２００で書き込む場合、入力編集作業として秘密鍵を設定するのと同じタイミングでの設定が考えられ、基本的に番号体系はシステムとして予め決定されていて、発行機２００としてもその体系のデータを書き込む様にプログラムされているものとして、使用する（発行する）番号を指定するだけの場合や、直接キーボード等から入力する場合等がある。

【００９８】続いて、図１６を参照して第３の実施形態について説明する。図１６は、この発明の第３の実施形態に係るＩＣカード処理システムを示す図である。

【００９９】この第３の実施形態では、第１及び第２の実施形態で説明したセキュリティをより強固なものとするため、秘密鍵をカード個別番号から生成する。

【０１００】例えば、発行機２００と交換機５００の双方に認証子生成用秘密鍵の生成ロジックと秘密鍵生成鍵Ｋ’を設定し、この秘密鍵生成鍵Ｋ’とカード個別番号から認証子生成用秘密鍵の生成ロジックにより秘密鍵Ｋを生成する。すなわち、発行時にＩＣカード３００のメモリ３３０内に格納される秘密鍵Ｋは、発行機２００が内蔵する秘密鍵生成ロジックによりカード個別番号と秘密鍵生成鍵Ｋ’に従い生成され、書き込まれたものとなる。また、このＩＣカード３００を使用する際、交換機５００では、電話機４００経由でＩＣカード３００から受け取ったカード個別番号と交換機５００のメモリ５３０内の秘密鍵生成鍵Ｋ’から、メモリ５３０内の秘密生成ロジックを使用して秘密鍵を生成して認証子生成に使用する。

【０１０１】これにより、カードに格納する秘密鍵は全てのカードで異なる値となり、システムの解析がより困難になる。

【０１０２】なお、この場合発行機２００と交換機５００双方に認証子生成用秘密鍵の生成ロジックと秘密鍵生成鍵Ｋ’を持たせる必要があるが、その方法としてそれぞれの製造段階での制御プログラムに包含させておく事が考えられる。また、このような秘密鍵Ｋを以下、個別秘密鍵と称する。

【０１０３】さらに、この第３の実施形態では、第１及び第２の実施形態で説明したセキュリティをより強固なものとするため、秘密鍵生成鍵を複数組用意し、個別秘密鍵を複数組生成し、各個別秘密鍵を対応させて使用する。

【０１０４】例えば、発行機２００と交換機５００の双方に個別秘密鍵の生成ロジックと複数の秘密鍵生成鍵Ｋ’１、Ｋ’２、…、Ｋ’ｎ、…、Ｋ’Ｎを持ち、カード個別番号から複数の個別秘密鍵Ｋ１、Ｋ２、…、Ｋｎ、…、ＫＮを生成する。

【０１０５】すなわち、ＩＣカード３００に格納する個別秘密鍵Ｋｎは、カード発行時にカード個別番号と秘密鍵生成鍵Ｋ’ｎから発行機２００が内蔵する秘密鍵生成ロジックを使用して生成してカードへ書き込む。また、そのＩＣカード３００を使用する際、交換機５００では電話機４００経由でＩＣカード３００から受け取ったカード個別番号と交換機５００のメモリ５３０内の秘密鍵生成鍵Ｋ’ｎから、メモリ５３０内の秘密鍵生成ロジックを使用して個別秘密鍵Ｋｎを生成して認証子生成に使用する。運用で都度使用されるｎは第２の実施形態と同様に決定される。

【０１０６】また、交換機５００側での秘密鍵管理はＩＣカード３００に格納されているＫ’１～Ｋ’Ｎ全てを当初から制御プログラムに包含しておき、そのいずれを適用するかを選択する方法と、常に１種類だけ保持し都度入れ替え（書き換え）る方式が考えられる。

【０１０７】これにより、ＩＣカード３００に格納する複数の個別秘密鍵は全てのカードで異なる値の組となり、システムの解析がより困難になる。

【０１０８】またさらに、この第３の実施形態では、第１及び第２の実施形態で説明したセキュリティをより強固なものとするため、各秘密鍵生成鍵ごとに異なる秘密鍵生成ロジックを適用し、単一の秘密鍵生成鍵で複数の異なる個別秘密鍵を生成する。

【０１０９】例えば、発行機２００と交換機５００の双方に複数の認証子生成用秘密鍵の生成ロジックＬ１、Ｌ２、…、Ｌｎ、…、ＬＮと単一の秘密鍵生成鍵Ｋ’を持ち、カード個別番号から複数の個別秘密鍵Ｋ１、Ｋ２、…、Ｋｎ、…ＫＮを生成する。

【０１１０】すなわちＩＣカード３００に格納する個別秘密鍵Ｋｎは、カード発行時にカード個別番号と秘密鍵生成鍵Ｋ’から発行機２００が内蔵する秘密鍵生成ロジックＬｎを使用して生成してカードへ書き込む。また、そのカードを使用する際、交換機５００では電話機４００経由でＩＣカード３００から受け取ったカード個別番号と交換機５００のメモリ５３０内の秘密鍵生成鍵Ｋ’から、５３０内の秘密鍵生成ロジックＬｎを使用して個別秘密鍵Ｋｎを生成して認証子生成に使用する。運用で都度使用されるｎは他の実施形態と同様に決定される。

【０１１１】また、交換機５００側での秘密鍵管理はカードに格納されているＫ１～ＫＮを生成する秘密鍵生成鍵Ｋ’と生成ロジックＬ１～Ｌｎ全てを当初から制御プログラムに包含しておき、いずれのＬｎを適用するかを選択する方法と、Ｋ’と１種類のＬｎだけを常に保持し都度入れ替え（書き換え）る方式が考えられる。また発行機２００についても秘密鍵生成鍵Ｋ’と認証子生成用秘密鍵の複数の生成ロジックとを持つ必要があるが、その方法として製造段階での制御プログラムに包含させておく事が考えられる。

【０１１２】これにより、ＩＣカード３００に格納する複数の個別秘密鍵は全てのカードでより複雑な関係を持った異なる値の組となり、システムの解析がより困難になる。

【０１１３】さらにまた、この第３の実施形態では、第１及び第２の実施形態で説明したセキュリティをより強固なものとするため、異なる秘密鍵生成鍵ごとに異なる秘密鍵生成ロジックを適用し異なる個別秘密鍵を生成する。

【０１１４】例えば、発行機２００と交換機５００の双方に複数の認証子生成用秘密鍵の生成ロジックＬ１、Ｌ２、…、Ｌｎ、…、ＬＮと各Ｌｎに対応する秘密鍵生成

鍵K’ｎを持ち、カード個別番号から複数の個別秘密鍵を生成する。

【０１１５】すなわちカードに格納する個別秘密鍵Ｋｎは、カード発行時にカード個別番号と秘密鍵生成鍵K’ｎから発行機２００が内蔵する秘密鍵生成ロジックＬｎを使用して生成してＩＣカード３００へ書き込む。また、そのＩＣカード３００を使用する際、交換機５００では電話機４００経由でＩＣカード３００から受け取ったカード個別番号と交換機５００のメモリ５３０内の秘密鍵生成鍵K’ｎから、メモリ５３０内の秘密鍵生成ロジックＬｎを使用して個別秘密鍵Ｋｎを生成して認証子生成に使用する。運用で都度使用されるｎは他の実施形態と同様に決定される。

【０１１６】また、交換機５００側での秘密鍵管理はＩＣカード３００に格納されているＫ１～ＫＮを生成する秘密鍵生成鍵K’ｎと生成ロジックＬ１～Ｌｎ全てを当初から制御プログラムに包含しておき、いずれのＬｎを適用するかを選択する方法と、１種類のK’ｎと１種類のＬｎだけを常に保持し都度入れ替え（書き換え）る方式が考えられる。また発行機２００についても複数の秘密鍵生成鍵K’ｎと認証子生成用秘密鍵の複数の生成ロジックＬｎとを持つ必要があるが、その方法として製造段階での制御プログラムに包含させておく事が考えられる。

【０１１７】これにより、ＩＣカード３００カードに格納する複数の個別秘密鍵は全てのＩＣカード３００でより複雑な関係を持った異なる値の組となり、システムの解析がより困難になる。

【０１１８】このような第３の実施形態のＩＣカード処理システムにおけるセキュリティは次のようにして守られる。

【０１１９】まず、製造設備１００で認証子生成関数を含むカード制御プログラムがＩＣカード３００へ登録される。さらに、発行機２００でカード個別番号、度数、及び複数の個別秘密鍵１～Ｎがカードへ登録される。個別秘密鍵１～Ｎは、発行機２００のメモリ２３０内のカード個別番号と複数の秘密鍵生成鍵１～Ｎを基にして対応する複数の秘密鍵生成関数１～Ｎにより生成されたものである。

【０１２０】例えば、電話機４００にＩＣカード３００が差し込まれると、電話機４００はメモリ４３０内の乱数生成関数を使用して、メモリ４３０内の電話機番号と時計回路４４０から取得される日時データから乱数を生成しカードへ送る。因みに、時計回路４４０から取得される日時情報は取得の都度異なる値となるため、乱数も都度異なる値として生成される。

【０１２１】電話機４００で生成された乱数を受け取ったカード３００側では、メモリ３３０内の認証子生成関数を使用して、電話機で生成された乱数、メモリ３３０内の個別秘密鍵ｎ及び度数情報から認証子を生成する。生成された認証子は、メモリ３３０内の度数情報及びカード個別番号とともに電話機４００へ送られる。

【０１２２】ＩＣカード３００からの度数情報、カード個別番号、及び認証子を受け取った電話機４００は、これら度数情報、カード個別番号、及び認証子を、先に生成しＩＣカード３００へ送った乱数とともに交換機５００へ送る。

【０１２３】交換機５００は、メモリ５３０内の秘密鍵生成関数ｎと秘密鍵生成鍵ｎを使用して、電話機４００に差し込まれたカードに対応する個別秘密鍵ｎを生成する。そして、この生成された個別秘密鍵ｎとメモリ５３０内の認証子生成関数により、電話機４００から受け取られた度数情報及び電話機４００が生成した乱数から交換機独自に認証子を生成する。さらに、交換機５００は、比較部５４０において交換機５００自身で生成された認証子と、電話機４００経由で送られてきた認証子とを比較する。そして、通話可否判定部５５０において、比較結果から電話機４００に差し込まれたＩＣカードによる通話の可否判定が下される。例えば、自身で生成された認証子と電話機４００経由で送られてきた認証子とが一致すれば、電話機４００に差し込まれたＩＣカードによる通話が許可され、回線が接続される。

【０１２４】ある個別秘密鍵による運用が一定期間継続した場合や、個別秘密鍵漏洩の懸念が発生した場合、交換機５００から電話機４００経由で個別秘密鍵変更コマンドが送られ、以降運用に適用される個別秘密鍵が変更される。個別秘密鍵が変更されるということは、秘密鍵生成鍵及び秘密鍵生成関数が変更されるということである。

【０１２５】最後に、図１７～図２２を参照して、上記説明した機器による運用の際のＩＣカード３００～電話機４００～交換機５００の間で交換される通信電文の形式と内容について説明する。

【０１２６】これらの電文は電話機４００が独自にＩＣカード３００とやりとりする場合と、電話機４００が交換機５００とＩＣカード３００のやりとりを仲介するだけの場合がある。

【０１２７】ＩＣカード３００は通常外部からの命令に従って動作する。つまり外部からの命令電文を受け取り、それに応える形で応答電文を返す動作が基本となる。図１７は、それら命令電文と応答電文双方に共通な電文の全体形式を示している。電文全体としてはその命令、応答の内容を示す本体部を伝送制御情報が挟む形となる。

【０１２８】図１８～図２２は、この命令、応答の内容を示す本体部の形式内容についてのものである。

【０１２９】基本的に本体部は命令電文については命令内容をコード情報として始めに示し、以降その命令実行に必要な情報が付加される。また、応答電文は指示された命令内容の実行結果を示すコード情報を始めに示し、

以降その命令の実行結果として伝える必要のある情報が付加される。

【０１３０】図１８はキー照合電文の本体部を示しており、前記の例では発行機２００の設定用カードから秘密鍵を読み出す際の照合用キーの照合に使用する。

【０１３１】図１９はデータ書き込み電文の本体部であり、前記の例では発行機２００でＩＣカード３００を発行する際のＩＣカード３００への各種データ書き込みに使用する。

【０１３２】図２０はデータ書き込み電文の本体部を示しており、前記の例では運用の中で電話機４００がＩＣカード３００から各種データを読み出す際に使用する。

【０１３３】図２１は認証子生成電文の本体部を示しており、前記の例では運用の中で電話機４００がＩＣカード３００に対して乱数を渡して認証子を生成させる際に使用する。

【０１３４】図２２は秘密鍵変更電文の本体部を示しており、運用に適用する秘密鍵を変更する際にＩＣカード３００に対して今後どのキーを適用するかを指示して変更させる際に使用する。

【０１３５】

【発明の効果】この発明によれば、セキュリティの要となる秘密情報（秘密鍵等）が漏洩しにくく、また、このような秘密情報が漏洩した場合でも、漏洩した秘密情報による不正使用を防止できるＩＣカード処理システムを提供することができる。

【図面の簡単な説明】

【図１】ＩＣカードの外観を示す図。

【図２】ＩＣカードの製造手順を示すフローチャート。

【図３】ＩＣチップの概略構成を示す図。

【図４】発行機の外観を示す図。

【図５】発行機によるＩＣカードの発行を説明するフローチャート。

【図６】設定用ＩＣカードを説明するための図。

【図７】設定用ＩＣカードを説明するための図。

【図８】設定用ＩＣカードを説明するための図。

【図９】相互認証を説明するための図。

【図１０】電話機の外観を示す図。

【図１１】電話機の製造手順を示すフローチャート。

＊【図１２】交換機の外観を示す図。

【図１３】交換機の製造手順を示すフローチャート。

【図１４】この発明の第１の実施形態に係るＩＣカード処理システムを示す図。

【図１５】この発明の第２の実施形態に係るＩＣカード処理システムを示す図。

【図１６】この発明の第３の実施形態に係るＩＣカード処理システムを示す図。

【図１７】ＩＣカードの電文の全体形式の概略を示す図。

【図１８】キー照合電文の本体部の概略を示す図。

【図１９】データ書き込み電文の本体部の概略を示す図。

【図２０】データ読み出し電文の本体部の概略を示す図。

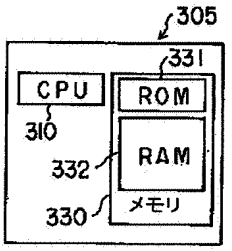
【図２１】認証子生成電文の本体部の概略を示す図。

【図２２】適用秘密鍵変更電文の本体部の概略を示す図。

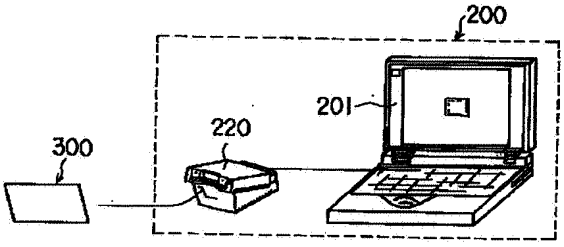
【符号の説明】

２００…発行機
２１０…発行機ＣＰＵ
２２０…カードリーダ・ライタ
２３０…メモリ
３００…ＩＣカード
３１０…ＩＣカードＣＰＵ
３２０…インターフェイス
３３０…メモリ
４００…電話機
４１０…電話機ＣＰＵ
４２０…インターフェイス
４３０…メモリ
４４０…時計回路
５００…交換機
５１０…交換機ＣＰＵ
５２０…インターフェイス
５３０…メモリ
５４０…比較部
５５０…通話可否判定部

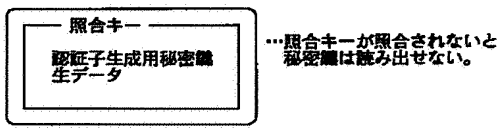
【図３】



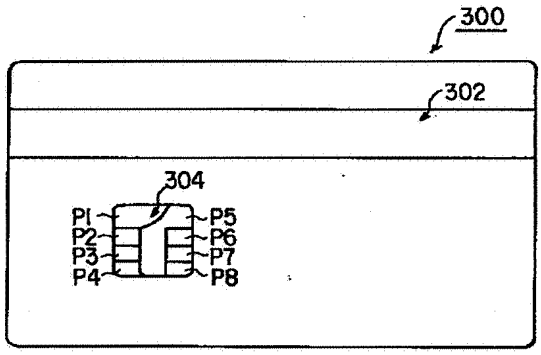
【図４】



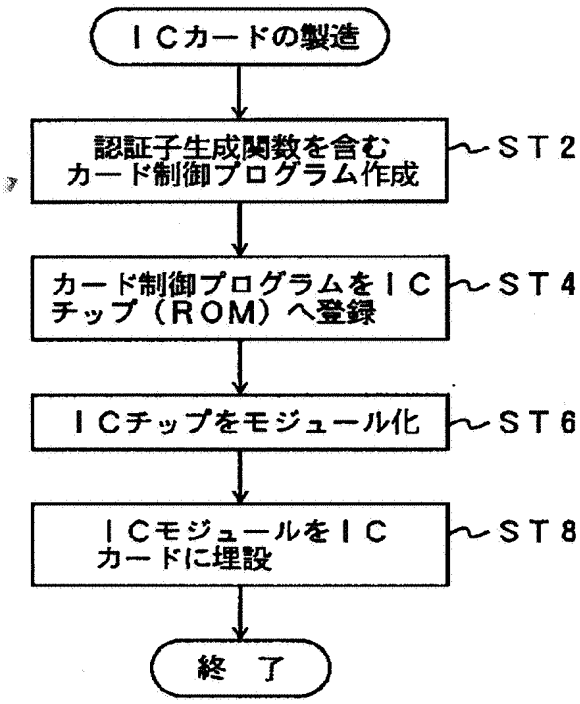
【図６】



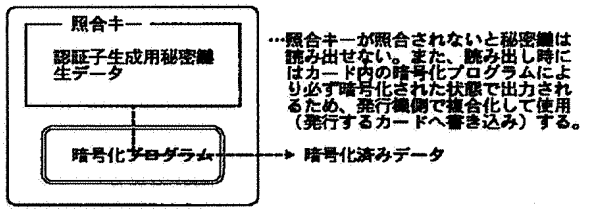
【図１】



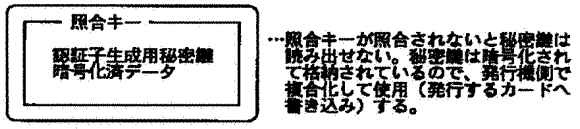
【図２】



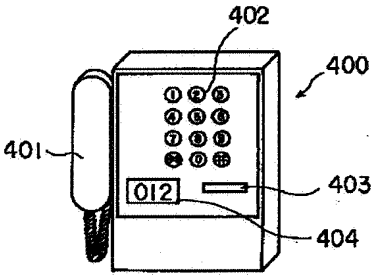
【図７】



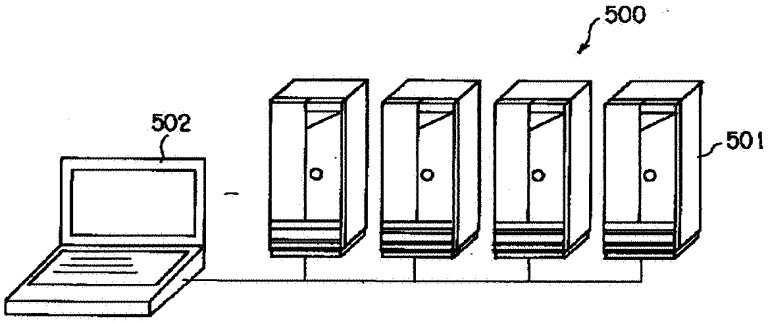
【図８】



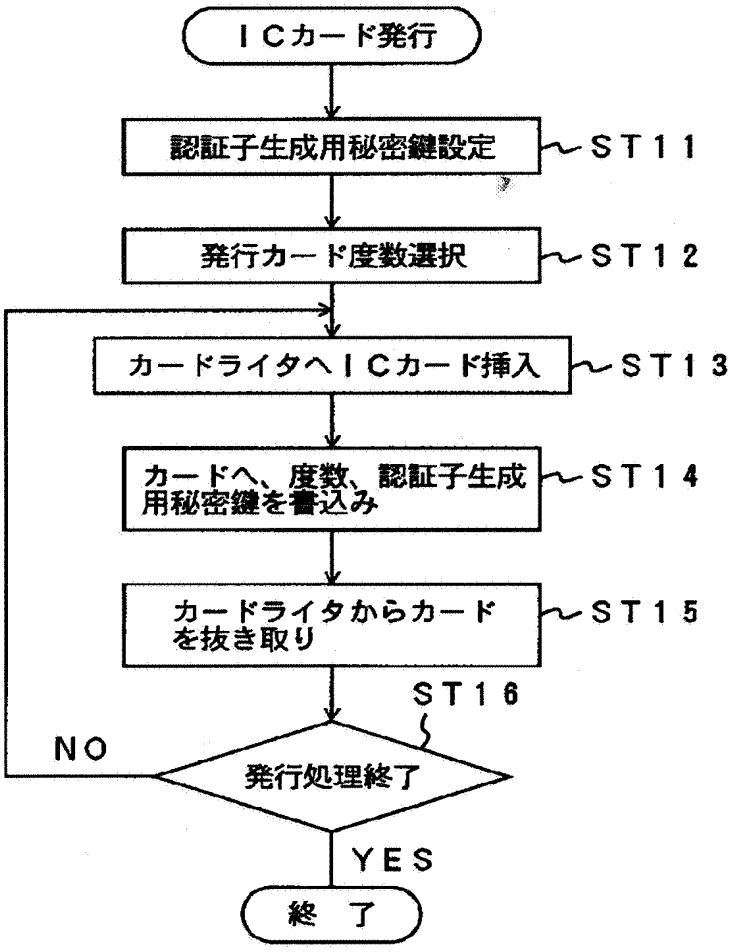
【図１０】



【図１２】



【図５】



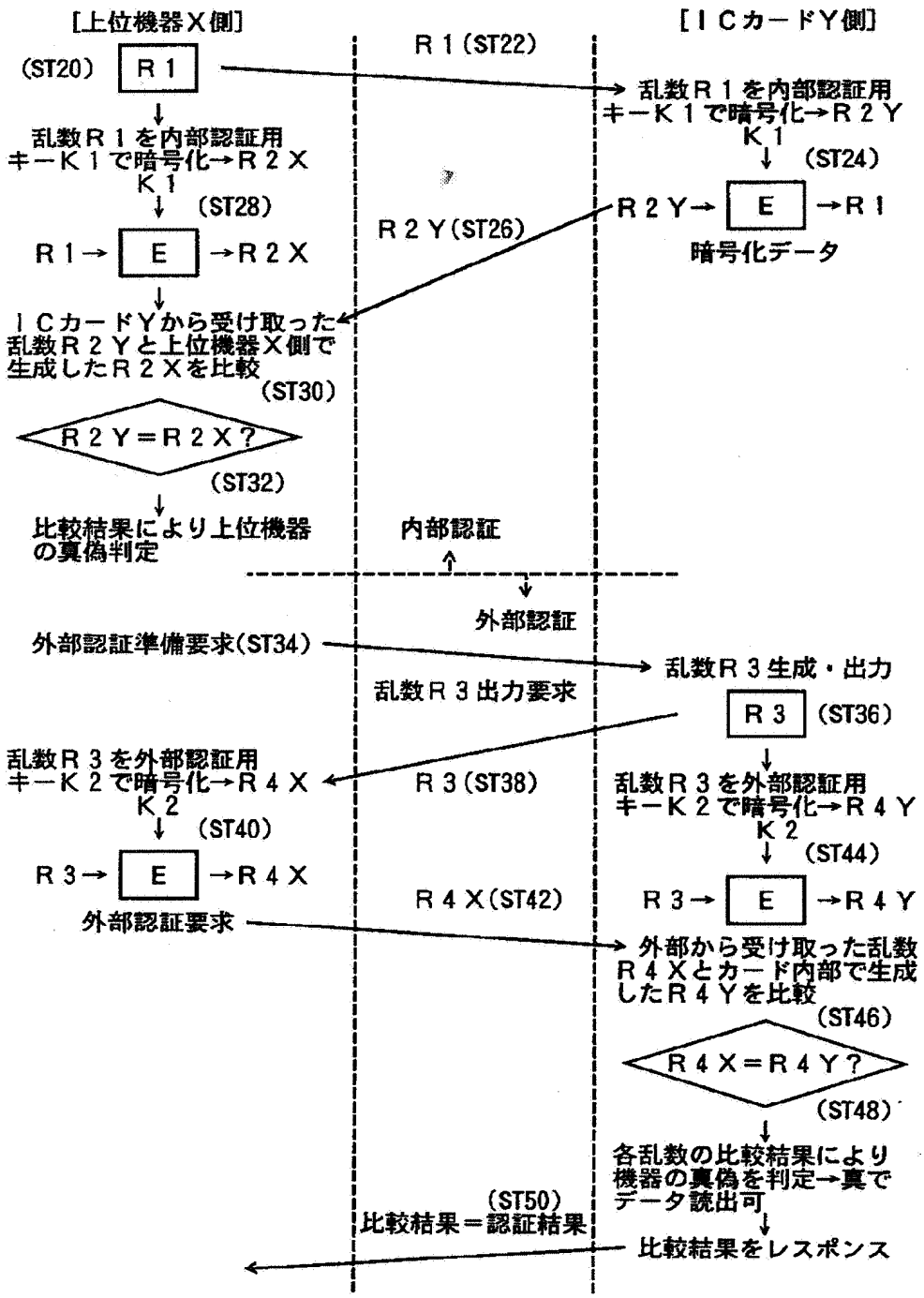
【図１７】

送信元識別符号	送信先識別符号	本体部データ長	[本体部]	誤り検出信号

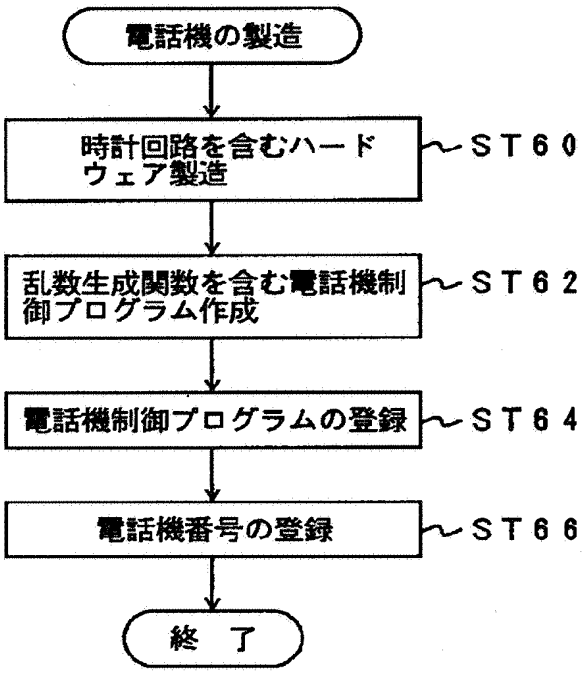
【図１８】

命令電文：	キー照合命令コード	照合対象キー識別子	照合キー値
応答電文：	照合結果表示コード		

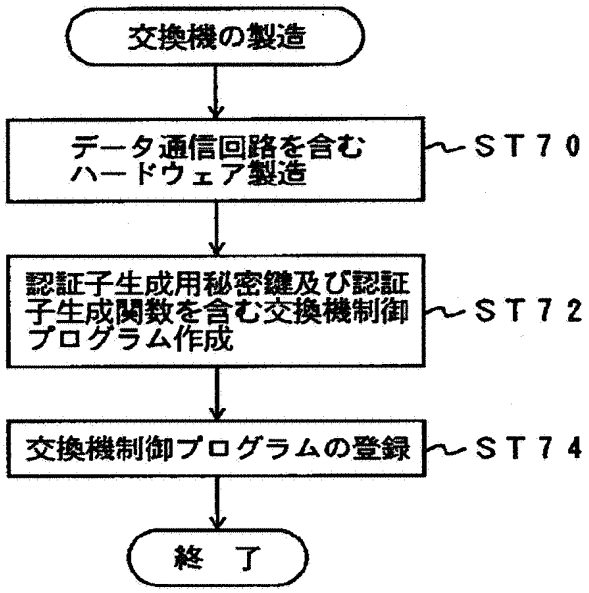
【図９】


[上位機器Ｘ側]
[ＩＣカードＹ側]
(ST20)
Ｒ１
Ｒ１(ST22)
乱数Ｒ１を内部認証用キーＫ１で暗号化→Ｒ２Ｙ
Ｋ１
(ST24)
Ｒ２Ｙ→ Ｅ →Ｒ１
暗号化データ
Ｒ２Ｙ(ST26)
乱数Ｒ１を内部認証用キーＫ１で暗号化→Ｒ２Ｘ
Ｋ１
(ST28)
Ｒ１→ Ｅ →Ｒ２Ｘ
ＩＣカードＹから受け取った乱数Ｒ２Ｙと上位機器Ｘ側で生成したＲ２Ｘを比較
(ST30)
Ｒ２Ｙ＝Ｒ２Ｘ？
(ST32)
比較結果により上位機器の真偽判定
内部認証
外部認証
外部認証準備要求(ST34)
乱数Ｒ３生成・出力
乱数Ｒ３出力要求
Ｒ３
(ST36)
乱数Ｒ３を外部認証用キーＫ２で暗号化→Ｒ４Ｘ
Ｋ２
(ST40)
Ｒ３→ Ｅ →Ｒ４Ｘ
Ｒ３(ST38)
乱数Ｒ３を外部認証用キーＫ２で暗号化→Ｒ４Ｙ
Ｋ２
(ST44)
Ｒ３→ Ｅ →Ｒ４Ｙ
Ｒ４Ｘ(ST42)
外部認証要求
外部から受け取った乱数Ｒ４Ｘとカード内部で生成したＲ４Ｙを比較
(ST46)
Ｒ４Ｘ＝Ｒ４Ｙ？
(ST48)
各乱数の比較結果により機器の真偽を判定→真でデータ読出可
(ST50)
比較結果＝認証結果
比較結果をレスポンス

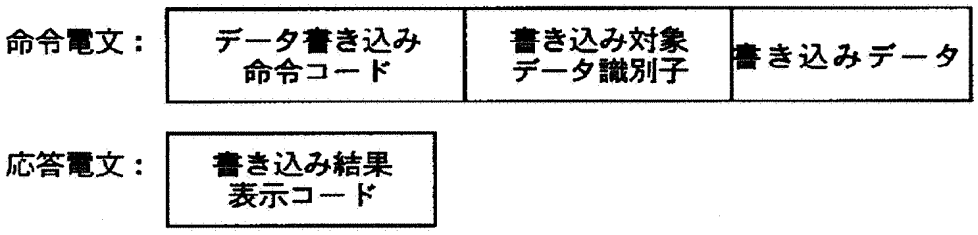
【図１１】



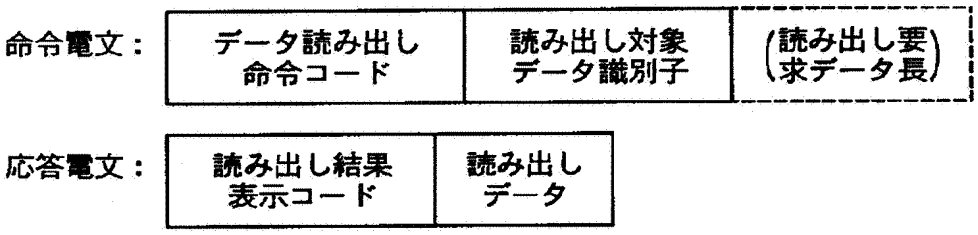
【図１３】



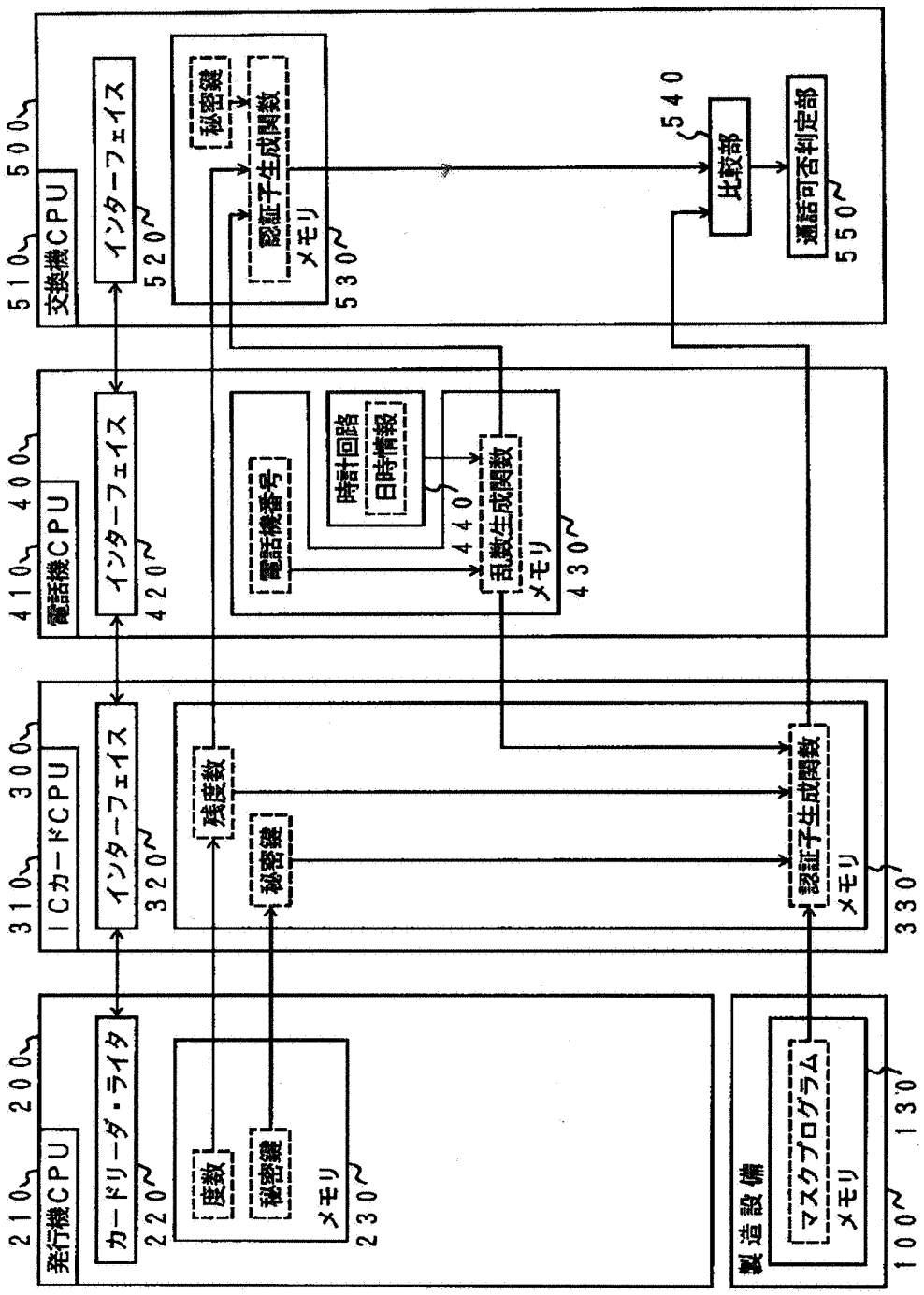
【図１９】



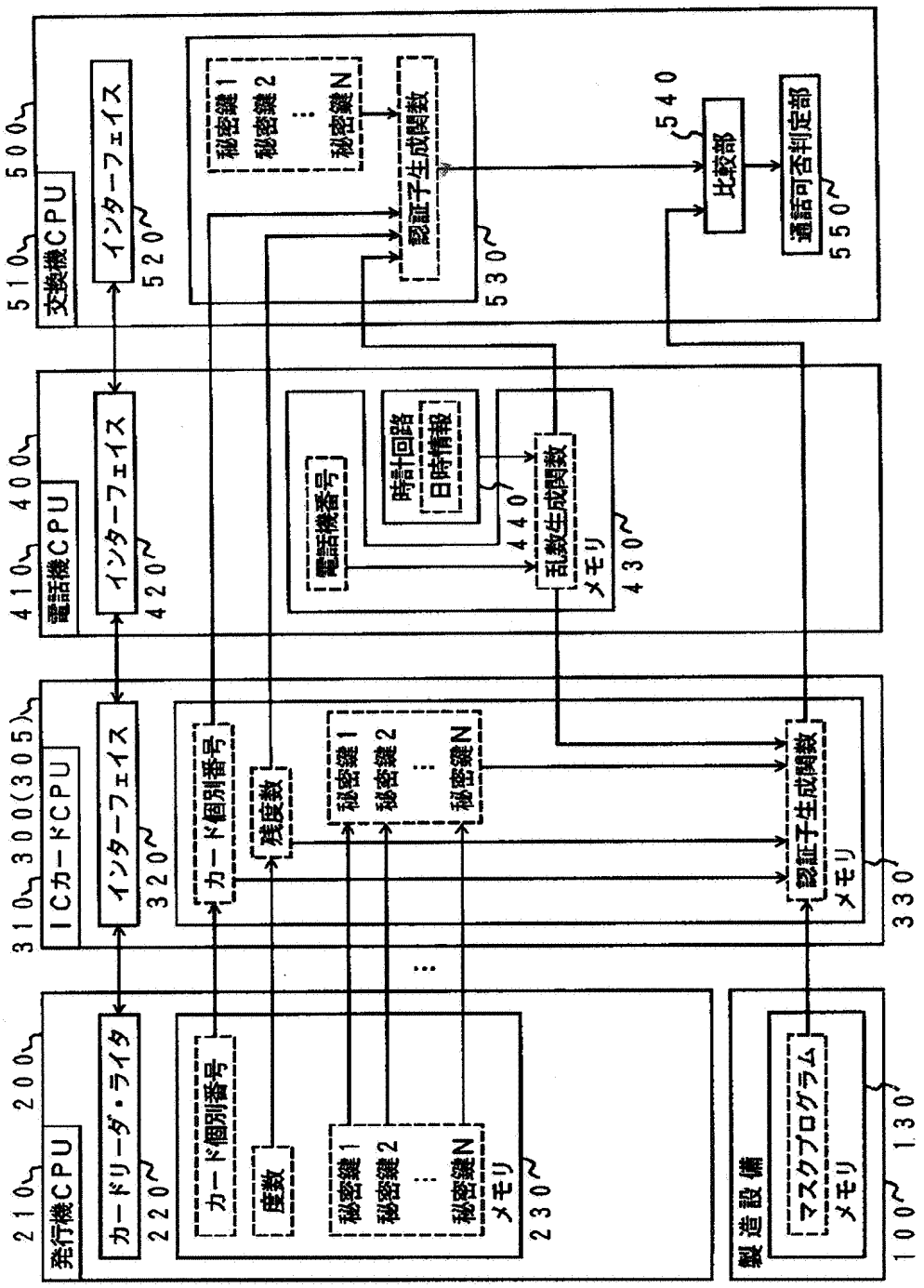
【図２０】



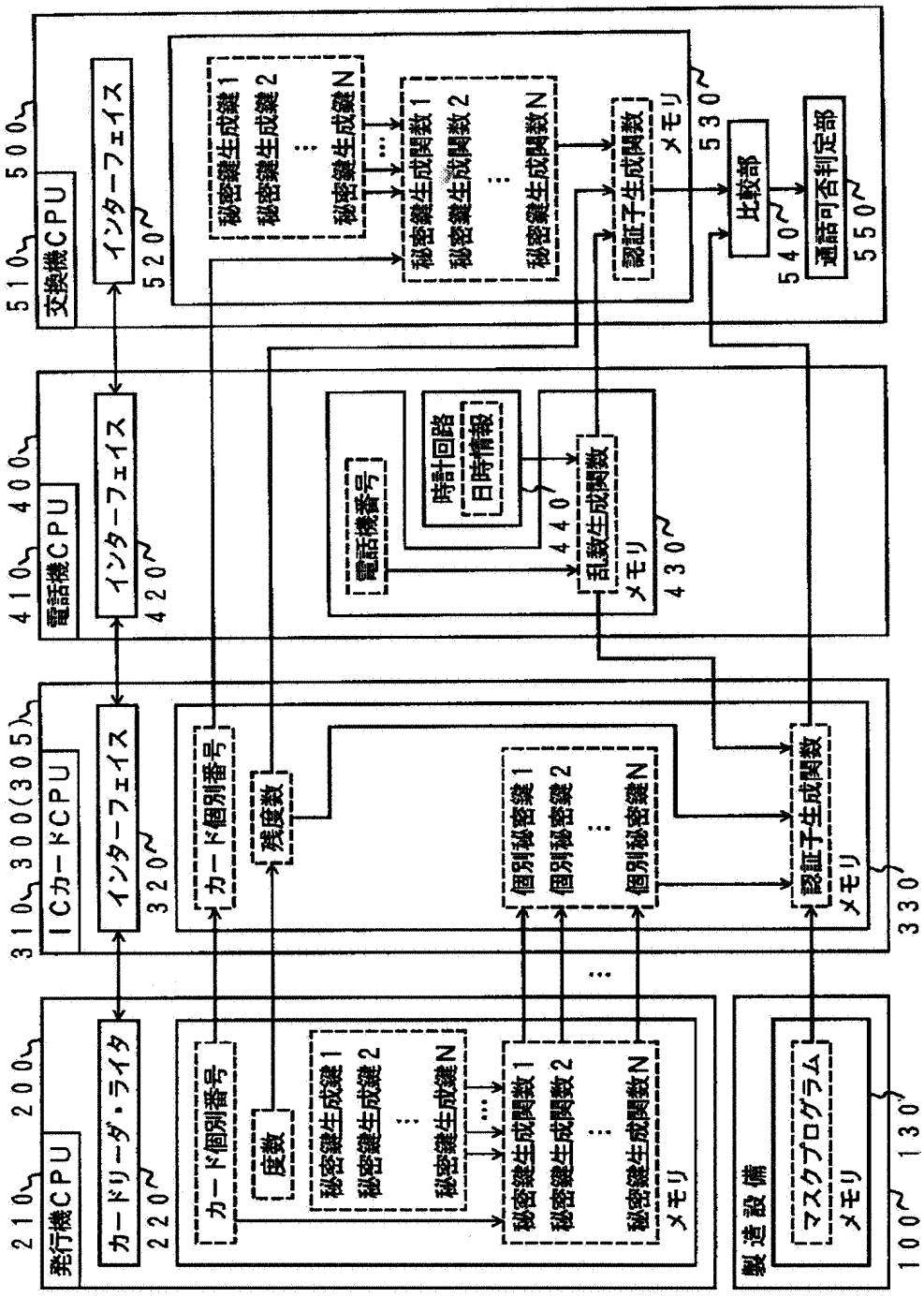
【図１４】


発行機CPU
210
200
カードリーダ・ライタ
220
度数
秘密鍵
メモリ
230
ICカードCPU
310
300
インターフェイス
320
残度数
秘密鍵
電話機CPU
410
400
インターフェイス
420
電話機番号
時計回路
日時情報
440
乱数生成関数
メモリ
430
交換機CPU
510
500
インターフェイス
520
秘密鍵
認証子生成関数
メモリ
530
540
比較部
通話可否判定部
550
製造設備
100
130
マスクプログラム
メモリ
認証子生成関数
メモリ
330

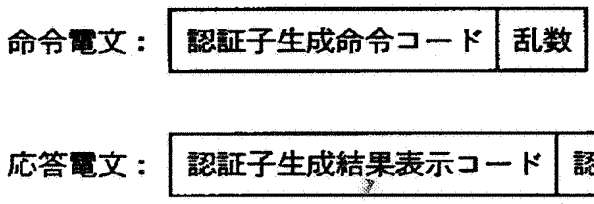
【図１５】


発行機CPU
210
200
カードリーダ・ライタ
220
カード個別番号
座数
秘密鍵1
秘密鍵2
秘密鍵N
メモリ
230
ICカードCPU
310
300(305)
インターフェイス
320
カード個別番号
残度数
秘密鍵1
秘密鍵2
秘密鍵N
認証子生成関数
メモリ
330
電話機CPU
410
400
インターフェイス
420
電話機番号
時計回路
日時情報
440
乱数生成関数
メモリ
430
交換機CPU
510
500
インターフェイス
520
秘密鍵1
秘密鍵2
秘密鍵N
認証子生成関数
530
540
比較部
通話可否判定部
550
製造設備
マスクプログラム
メモリ
100
130

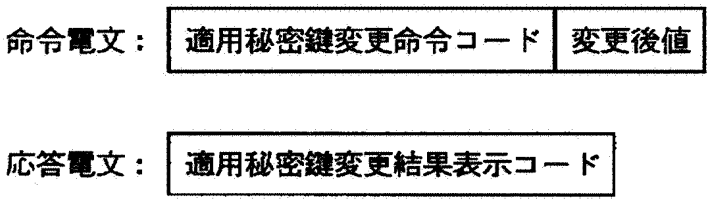
【図１６】


発行機CPU
210
200
カードリーダ・ライタ
220
カード個別番号
度数
秘密鍵生成鍵1
秘密鍵生成鍵2
秘密鍵生成鍵N
秘密鍵生成関数1
秘密鍵生成関数2
秘密鍵生成関数N
メモリ
ICカードCPU
310
300(305)
インターフェイス
320
カード個別番号
残度数
個別秘密鍵1
個別秘密鍵2
個別秘密鍵N
認証子生成関数
メモリ
330
電話機CPU
410
400
インターフェイス
420
電話機番号
時計回路
日時情報
440
乱数生成関数
メモリ
430
交換機CPU
510
500
インターフェイス
520
秘密鍵生成鍵1
秘密鍵生成鍵2
秘密鍵生成鍵N
秘密鍵生成関数1
秘密鍵生成関数2
秘密鍵生成関数N
認証子生成関数
メモリ
530
比較部
540
通話可否判定部
550
製造設備
マスクプログラム
メモリ
100
130

【図２１】



【図２２】



フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｍ	15/00		Ｇ０６Ｋ	19/00	Ｒ
	17/02				Ｕ